POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Auditorias de Cibersegurança para PME: Uma Abordagem Prática e Simplificada

Tomás Alexandre dos Santos Oliveira

Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

Leiria, Agosto 2025

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Auditorias de Cibersegurança para PME: Uma Abordagem Prática e Simplificada

Tomás Alexandre dos Santos Oliveira 2230462

Orientador: Professora Doutora Marisa Maximiano

Orientador: Professor Ricardo Gomes

Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

Projeto

Leiria, Agosto 2025

Agradecimentos

Agradeço aos meus orientadores, Professora Doutora Marisa Maximiano e Professor Ricardo Gomes, pela orientação e pelo apoio contínuo em cada etapa deste projeto. A vossa disponibilidade e os vossos conselhos foram cruciais para a concretização deste trabalho.

Resumo

A crescente digitalização expõe as Pequenas e Médias Empresas (PME) a ciberameaças cada vez mais complexas e sofisticadas. No entanto, estas organizações enfrentam desafios significativos, como a escassez de recursos e a complexidade das normas e *frameworks* de cibersegurança existentes, que dificultam a adoção de boas práticas. Este projeto nasce para colmatar esta lacuna, propondo uma estrutura de auditoria prática, acessível e adaptada à realidade das PME.

Para isso, foi desenvolvida uma metodologia estruturada para a criação de um roteiro de auditoria, adaptado às necessidades das PME e centrado nos controlos mais essenciais do Quadro Nacional de Referência para a Cibersegurança (QNRCS). Complementarmente, foi elaborado um manual do auditor, que serve como guia prático e sistemático, e uma aplicação *web* de suporte à auditoria, centralizando a gestão e visualização dos resultados.

A validade e a eficácia da abordagem foram comprovadas através de um caso de estudo prático numa PME do setor tecnológico. Este estudo de caso demonstrou que a metodologia é clara e o manual um guia eficaz. A aplicação *web* funcionou como a peça-chave, tornando o processo de auditoria intuitivo, centralizado e com resultados práticos imediatos.

A principal contribuição deste trabalho reside na capacidade de transformar a complexidade da auditoria de cibersegurança num processo objetivo e acionável para as PME. Ao centralizar a recolha de dados, automatizar cálculos de risco e apresentar resultados de forma clara e visual, a solução otimiza o trabalho do auditor e capacita o cliente a compreender a sua postura de segurança, facilitando a priorização de medidas corretivas. Em suma, este projeto torna a segurança digital mais acessível, preparando as organizações para enfrentarem os desafios do ciberespaço de forma mais resiliente e informada.

Palavras-Chave: Cibersegurança, Auditorias, Pequenas e Médias Empresas, QNRCS.

Abstract

Increasing digitalization exposes Small and Medium-sized Enterprises (SME) to increasingly complex and sophisticated cybersecurity threats. However, these organizations face significant challenges, such as resource scarcity and the complexity of existing cybersecurity standards and frameworks, which hinder the adoption of effective practices. This project aims to bridge this gap by proposing a practical, accessible, and adaptable audit structure tailored to the reality of SMEs.

To achieve this, a structured methodology was developed for creating an audit roadmap, customized to SME needs and focused on the most essential controls of National Cybersecurity Reference Framework (QNRCS). Additionally, a detailed auditor's manual was prepared, serving as a practical and systematic guide, alongside a supporting web application to centralize audit management and results visualization.

The validity and effectiveness of this approach were demonstrated through a practical case study conducted in a technology sector SME. This case showed the methodology to be clear and the manual an effective guide. The web application proved to be the key component, making the audit process intuitive, centralized, and yielding immediate practical results.

The main contribution of this work lies in its ability to transform the complexity of cybersecurity audits into an objective and actionable process for SMEs. By centralizing data collection, automating risk calculations, and presenting results clearly and visually, the solution optimizes the auditor's work and empowers clients to understand their security posture, thereby facilitating the prioritization of remediation actions. In summary, this project makes digital security more accessible, preparing organizations to address cyberspace challenges in a more resilient and informed manner.

Keywords: Cybersecurity, Audits, Small and Medium-sized Enterprises, QNRCS.

Conteúdo

Lista de Figuras

Lista de Tabelas

Siglas

ASMAS *Adaptable Security Maturity Assessment and Standardization*. (*p. 23, 24*)

CGI *Common Gateway Interface*. (*p. 95*)
CIA *Confidentiality, Integrity, Availability*. (*p. 6, 15, 19, 27*)
CIS *Center for Internet Security*. (*p. vii, 4, 9, 14, 19, 20, 26, 30*)
CIS *Controls* *CIS Critical Security Controls*. (*p. 3, 6, 9, 10, 35*)
CISO *Chief Information Security Officer*. (*p. 12*)
CNCS Centro Nacional de Cibersegurança. (*p. vii, 11–14*)
COBIT *Control Objectives for Information Technologies*. (*p. 26*)
CSAM *CyberSecurity Audit Model*. (*p. 4, 14, 17, 18*)
CSETA *CyberSecurity Education, Training, and Awareness*. (*p. 18*)
CSF *NIST Cybersecurity Framework*. (*p. vii, 2, 3, 6, 8, 9, 21, 25–27*)
CSIRT *Computer Security Incident Response Team*. (*p. 12*)
CVE *Common Vulnerabilities and Exposures*. (*p. 51*)
CVSS *Common Vulnerability Scoring System*. (*p. 50–52, 61*)

DAST *Dynamic Application Security Testing*. (*p. 53*)
DDoS *Distributed Denial-of-Service*. (*p. 38*)
DoD *Department of Defense*. (*p. 27*)

ECSF *European Cybersecurity Skills Framework*. (*p. vii, 11, 12*)
ENISA *European Union Agency for Cybersecurity*. (*p. vii, 11, 12, 30*)
EPSS *Exploit Prediction Scoring System*. (*p. 61*)

HIBP *Have I Been Pwned?*. (*p. 60*)

IEC *International Electrotechnical Commission*. (*p. iv–vi, 2–4, 6–8, 16, 17, 21, 22, 25–28, 30, 34–36, 38–40, 43, 86*)
IoT *Internet of Things*. (*p. 94*)
IP *Internet Protocol*. (*p. 24*)
ISO *International Organization for Standardization*. (*p. iv–vi, 2–4, 6–8, 14, 16, 17, 21, 22, 25–28, 30, 34–36, 38–40, 43, 86*)

MITM *Man-in-the-middle*. (*p. 42*)

NCS *National Cybersecurity Strategy*. (*p. 17*)
NIST *National Institute of Standards and Technology*. (*p. iv, v, 2–6, 8, 14, 15, 21, 24–28, 30, 34, 36, 54, 59*)

OSINT *Open Source Intelligence*. (*p. 94*)
OWASP *The Open Worldwide Application Security Project*. (*p. 24*)

PDCA *Plan–Do–Check–Act*. (*p. 27*)
PME Pequenas e Médias Empresas. (*p. ii, 1, 21–26, 28–31, 37, 38, 42–44, 67, 77, 78*)

QNRCS Quadro Nacional de Referência para a Cibersegurança. (*p. ii, vi–ix, 11–13, 30, 35, 36, 38–40, 43, 45, 60, 75, 86, 87, 91–93*)

RAM *Risk Assessment Method*. (*p. 4, 14, 19, 20*)
RGPD Regulamento Geral sobre a Proteção de Dados. (*p. 10, 16, 22, 30, 56*)
RMF *Risk Management Framework*. (*p. 27*)

SAST *Static Application Security Testing*. (*p. 53*)
SGSI Sistema de Gestão da Segurança da Informação. (*p. 6–8, 16, 17, 25–27*)
SME *Small and medium-sized enterprise*. (*p. 30*)
SOC *Security Operations Center*. (*p. 12, 18*)
SRTM *Security Requirements Traceability Matrix*. (*p. 27*)
SSL *Secure Sockets Layer*. (*p. 94*)

TI Tecnologia da Informação. (*p. 4–7, 15, 22, 23, 27, 67*)

UE União Europeia. (*p. 11*)

1 Introdução

A crescente digitalização das operações empresariais, embora essencial para a inovação e competitividade, resultou numa exposição sem precedentes a um leque crescente e sofisticado de ciberameaças. Atualmente, 91% das organizações passam por algum processo de transformação digital, o que, por natureza, amplia a sua superfície de ataque [1]. Neste ecossistema interconectado, a cibersegurança deixa de ser um mero requisito técnico para se afirmar como um pilar fundamental para a continuidade e resiliência do negócio.

Face a este cenário, os dados estatísticos evidenciam uma realidade implacável, revelando que em 2023, 59% das organizações foram alvo de ataques de *ransomware*, uma ameaça que afeta de forma persistente até as empresas de menor dimensão [1]. O impacto financeiro é igualmente devastador, com o custo médio de uma violação de dados a atingir 4.45 milhões de dólares, um aumento de 15.3% desde 2020 [1]. A este paradigma de ameaças diretas, soma-se a crescente pressão regulatória, como o Regulamento Geral sobre a Proteção de Dados (RGPD), que impõe requisitos rigorosos e coimas significativas, demonstrando que a negligência em cibersegurança acarreta consequências legais e financeiras severas.

É neste contexto de risco elevado e de carência de recursos que a auditoria de cibersegurança emerge como uma ferramenta estratégica. Uma auditoria eficaz permite não só identificar vulnerabilidades e avaliar a conformidade das medidas de defesa existentes, mas também fornecer uma visão clara sobre a postura de segurança de uma organização. O presente projeto nasce da necessidade de colmatar a lacuna existente entre a complexidade das práticas de cibersegurança e a capacidade de implementação das Pequenas e Médias Empresas (PME), propondo uma estrutura de auditoria que é, simultaneamente, prática, acessível e adaptada à sua realidade.

1.1 Motivação e Objetivos

A cibersegurança representa um desafio particular para as PME. Estas organizações, que constituem a grande maioria do tecido empresarial português, enfrentam uma

dualidade de problemas que reside, por um lado, na notória falta de recursos, tanto financeiros como humanos, para investir em cibersegurança e, por outro, a complexidade intrínseca às normas e *frameworks* de referência, como a família ISO/IEC 27000 [2] ou o NIST CSF [3]. Tais *frameworks*, embora completas, são extensas e podem ser intimidadoras para equipas não especializadas, tornando difícil identificar por onde começar a implementação de controlos eficazes.

Esta dificuldade resulta em posturas de segurança frágeis, que não só colocam a própria empresa em risco, mas também os seus parceiros e clientes, uma vez que as PMEs são elos vitais em múltiplas cadeias de abastecimento. A motivação central deste trabalho é, portanto, desmistificar e simplificar o processo de avaliação da segurança, capacitando as PMEs a compreender e a melhorar a sua resiliência cibernética de forma autónoma e eficiente.

Para responder a esta necessidade, foram definidos os seguintes objetivos principais para este projeto:

1. Definir uma metodologia para a criação de um roteiro de auditoria, que seja adaptado às necessidades e ao contexto das PMEs, focando-se nos controlos mais relevantes e essenciais do Quadro Nacional de Referência para a Cibersegurança (QNRCS).
2. Elaborar um manual de auditor detalhado, que sirva como um guia prático e sistemático para a execução de cada fase da auditoria, garantindo a consistência e a qualidade do processo.
3. Desenvolver e validar uma aplicação *web* de suporte, que funcione como uma plataforma centralizada para a gestão da auditoria. Esta ferramenta permite ao auditor registar os seus achados e ao cliente consultar os resultados, visualizar as suas vulnerabilidades organizadas por nível de risco e compreender facilmente as ações prioritárias para a correção das mesmas.

Em suma, o projeto visa simplificar a segurança, transformando conceitos complexos num plano de ação claro e priorizado, que otimiza os recursos limitados das PMEs e promove uma cultura de melhoria contínua da segurança.

1.2 Resultados Esperados

A contribuição deste projeto resulta numa solução coesa e funcional que transforma a complexidade teórica das auditorias de cibersegurança num processo objetivo e tangível. Os resultados concretos materializam-se em três componentes interdependentes, cujo valor se manifesta tanto individualmente como em conjunto:

- Uma Metodologia de Auditoria Estruturada: O principal resultado é um roteiro claro que define o que avaliar e como o fazer no contexto de uma PME. Esta metodologia, baseada em *frameworks* reconhecidas mas adaptada à realidade nacional, permite uma avaliação de segurança focada e eficiente;

- Um Manual do Auditor Completo: Este manual servirá como um guia de referência essencial, padronizando o processo de auditoria e assegurando que todas as fases são executadas com rigor e consistência. Para o auditor, representa uma ferramenta que otimiza o seu trabalho, e para a organização auditada, garante a fiabilidade e a transparência da avaliação;
- Uma Aplicação Web de Suporte: A plataforma web é o resultado mais tangível, centralizando todo o fluxo da auditoria. Através dela, automatizam-se cálculos de risco, centraliza-se a recolha de dados e apresentam-se os resultados de forma visual e intuitiva.

Em conjunto, estes componentes oferecem um valor acrescido para o utilizador final. A PME obtém uma clareza sobre a sua postura de segurança real, recebe um plano de ação priorizado para a alocação eficiente de recursos, e dispõe de uma base de referência tangível para a melhoria contínua da sua maturidade em cibersegurança.

1.3 Estrutura do Documento

O presente documento está organizado de forma a guiar o leitor através de um percurso lógico, desde a fundamentação conceptual até à validação prática da solução proposta.

No Capítulo 2, são apresentados os Conceitos Relacionados, abordando os fundamentos da auditoria de segurança e detalhando as principais *frameworks* de cibersegurança (como a família ISO/IEC 27000, NIST CSF e CIS *Controls*) e os modelos relevantes para a realização de auditorias, que constituem a base teórica deste trabalho.

O Capítulo 3 oferece uma revisão dos Trabalhos Relacionados, explorando a literatura existente sobre os desafios de cibersegurança enfrentados pelas PMEs e as diferentes abordagens metodológicas para a implementação de controlos e avaliação de riscos.

No Capítulo 4, é detalhada a Metodologia de desenvolvimento do projeto, que se divide em três fases essenciais: Investigação, Desenvolvimento e Validação, explicando a abordagem seguida para atingir os objetivos propostos.

O Capítulo 5 constitui o núcleo do trabalho, descrevendo em pormenor o Desenvolvimento da solução. Este capítulo detalha a criação da metodologia do roteiro de auditoria, a elaboração do manual do auditor e o desenvolvimento da aplicação web de suporte.

No Capítulo 6, é apresentado o Caso de Estudo, onde a metodologia e as ferramentas desenvolvidas são aplicadas num cenário prático numa PME do setor tecnológico, validando a sua eficácia e viabilidade.

Finalmente, o Capítulo 7 apresenta as Conclusões, sintetizando os resultados alcançados, discutindo as contribuições e limitações do projeto, e propondo vertentes de investigação para trabalho futuro.

2
Conceitos Relacionados

Este capítulo apresenta os conceitos básicos da auditoria de segurança e explora a sua importância para o reforço da postura de segurança das organizações. Começa por discutir os princípios gerais da auditoria de segurança, incluindo os seus objetivos e impacto na gestão do risco. Em seguida, são discutidas as principais *frameworks* de cibersegurança, com ênfase nas metodologias amplamente utilizadas para proteger os ativos digitais. Por fim, são analisadas *frameworks* específicas e relevantes para a realização de auditorias de segurança, como o NIST SP 800-115, a ISO/IEC 27007:2020, o *CyberSecurity Audit Model* (CSAM) e o CIS *Risk Assessment Method* (RAM), destacando as suas aplicações práticas no fortalecimento da segurança organizacional.

2.1 Auditoria de Segurança

A auditoria de segurança de sistemas, conforme definido pela NIST SP 800-82r3 [4] e a ISO/IEC 7498-1:1994 [5], envolve a revisão e análise independentes dos registos e atividades de um sistema para determinar a adequação dos controlos de segurança, garantir o cumprimento da política de segurança estabelecida, detetar violações e recomendar alterações para contramedidas [6].

Este processo abrange uma vasta gama de tópicos, desde a auditoria do *data center* até à avaliação de sistemas específicos, como redes, servidores, aplicações e até ambientes em *cloud*. As auditorias de Tecnologia da Informação (TI) desempenham um papel crucial na verificação da segurança destes sistemas e aplicações. Avaliam as vulnerabilidades, asseguram a conformidade com as políticas internas e os requisitos regulamentares e avaliam a eficácia dos controlos de segurança implementados. O objetivo é confirmar que a postura de segurança da informação da organização é forte e resistente contra potenciais ameaças [7].

O processo de auditoria segue normalmente uma sequência estruturada de passos, conforme ilustrado na Figura 2.1, cada um projetado para recolher informações essenciais e avaliar de forma abrangente a postura de segurança de uma organização.

Embora existam várias abordagens distintas para estruturar uma auditoria de segu-

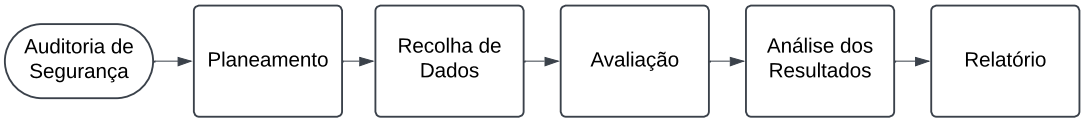

Figura 2.1: *Etapas do processo de auditoria de segurança*

rança, com pequenas diferenças entre si, as etapas descritas abaixo baseiam-se principalmente na metodologia descrita no NIST SP 800-115 [8]. Estas etapas garantem que a auditoria é completa, está alinhada com os objetivos de segurança e ajuda a identificar vulnerabilidades críticas e áreas que necessitam de reforço na postura de segurança [8, 9]:

- Planeamento da auditoria: A primeira etapa do processo de auditoria é o planeamento que envolve a definição dos objetivos da auditoria, como a análise dos controlos de segurança, a identificação de áreas vulneráveis e a verificação do cumprimento das políticas e requisitos de conformidade. Além disso, esta fase inclui a identificação dos sistemas, políticas e processos a serem auditados, bem como a determinação do âmbito. O âmbito pode incluir áreas específicas, como infra-estruturas de TI, controlos de segurança [10] ou mesmo departamentos específicos. A fase de planeamento também inclui a atribuição de recursos, como a equipa de auditoria e as ferramentas, e o desenvolvimento de um plano de auditoria [8] com metodologias claras;
- Recolha de dados: A fase seguinte do processo de auditoria centra-se na recolha de informações críticas sobre a infraestrutura da organização, as medidas de segurança [9], e as potenciais vulnerabilidades. Esta fase tem como objetivo proporcionar uma compreensão global do ambiente da rede e dos controlos de segurança existentes, bem como identificar quaisquer pontos fracos que possam representar riscos. A descoberta da rede desempenha um papel fundamental neste processo, ao permitir o mapeamento dos dispositivos, sistemas e ligações dentro da organização. Os controlos de segurança são, em seguida, identificados e mapeados. Além disso, é efetuada uma análise de vulnerabilidades para detetar falhas que possam ser exploradas;
- Avaliação dos controlos de segurança: Nesta fase, os auditores avaliam a eficácia dos controlos de segurança existentes. Estes podem incluir controlos de acesso, práticas de cifragem, gestão de incidentes de segurança e outras salvaguardas técnicas ou administrativas. A fase de avaliação verifica se estes controlos estão a funcionar como previsto, se estão em conformidade com as normas internas e externas, e se protegem adequadamente as informações sensíveis [9];
- Análise dos resultados: Depois de avaliarem os controlos de segurança, os auditores analisam os dados recolhidos para identificar eventuais falhas de conformidades ou vulnerabilidades. Isto inclui a verificação de que as medidas de segurança existentes cumprem os requisitos de conformidade necessários e a avaliação dos

riscos potenciais que podem afetar a organização. A análise ajuda a identificar áreas específicas que necessitam de atenção, tais como pontos fracos nos controlos ou práticas que podem não estar totalmente alinhadas com as normas da indústria ou com as políticas organizacionais [8];

- Relatório de auditoria: Após a análise, os auditores compilam as suas conclusões num relatório de auditoria. Este relatório descreve os riscos, falhas de conformidade e vulnerabilidades identificadas e inclui recomendações acionáveis. Estas recomendações podem incluir melhorias nos controlos existentes, a implementação de novas medidas de segurança ou alterações às políticas organizacionais para mitigar os riscos e melhorar a postura geral de segurança [8];
- Acompanhamento: A fase final do processo de auditoria consiste em garantir que as recomendações do relatório de auditoria são efetivamente implementadas. Isto pode incluir a realização de auditorias adicionais para verificar se as ações corretivas foram implementadas e se as melhorias foram integradas com sucesso na estrutura de segurança da organização. O processo de acompanhamento garante que as conclusões da auditoria são tratadas atempadamente e que a segurança se mantém sólida ao longo do tempo [8].

2.2 Principais *Frameworks* de Cibersegurança

As *frameworks* de cibersegurança desempenham um papel fundamental nas organizações e na implementação de políticas e práticas de segurança em ambientes empresariais e tecnológicos. Elas fornecem modelos estruturados para identificar, avaliar, proteger e responder a riscos de cibersegurança, além de promoverem a conformidade com regulamentos e melhores práticas globais. Nesta secção, são exploradas as principais *frameworks*, destacando a sua contribuição para a melhoria da segurança organizacional e para a proteção de sistemas e dados sensíveis. Serão exploradas normas reconhecidas internacionalmente, como a ISO/IEC 27000, o NIST CSF, o CIS *Controls* e outros modelos relevantes que fornecem um conjunto de diretrizes e controlos essenciais para mitigar ameaças cibernéticas e garantir a resiliência das infraestruturas de TI.

2.2.1 ISO/IEC da família 27000

A família de normas ISO/IEC 27000 [11] consiste num conjunto de normas internacionais desenvolvidas pela *International Organization for Standardization* (ISO) e pela *International Electrotechnical Commission* (IEC) para a gestão da segurança da informação. O principal objetivo desta família de normas é fornecer orientações e requisitos para estabelecer, implementar, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI). A segurança da informação refere-se à proteção de dados e informações, garantindo a sua Confidencialidade, Integridade e Disponibilidade (CIA).

A família ISO/IEC 27000 inclui uma série de normas que abrangem diferentes aspetos da gestão da segurança da informação, desde os requisitos gerais até às especifi-

cidades dos controlos e práticas de proteção da informação em vários contextos organizacionais. A norma central desta família é a ISO/IEC 27001 [12], que estabelece os requisitos para a implementação de um SGSI eficaz. Outras normas fornecem orientações adicionais ou especificam práticas que as organizações devem seguir.

Atualmente, existem várias normas no âmbito da família ISO/IEC 27000. Algumas das principais incluem:

- ISO/IEC 27001: Requisitos para um Sistema de Gestão da Segurança da Informação [12];
- ISO/IEC 27002: Controlos de segurança da informação [13];
- ISO/IEC 27005: Orientações sobre a gestão dos riscos de segurança da informação [14];
- ISO/IEC 27007: Diretrizes para a auditoria dos sistemas de gestão da segurança da informação [15].

Estas normas, juntamente com outras normas da família, formam um conjunto coeso que ajuda as organizações a adotarem uma abordagem estruturada para protegerem a sua informação, mitigarem os riscos e cumprirem os regulamentos e requisitos legais relacionados com a segurança da informação.

ISO/IEC 27001:2022

A ISO/IEC 27001:2022 [12] é uma das normas mais conhecidas no setor de TI e é amplamente reconhecida pela sua abordagem abrangente à segurança da informação e à cibersegurança. Ela estabelece os requisitos para a implementação de um SGSI, que inclui uma série de controlos de segurança concebidos para proteger as organizações contra ciberameaças. A adoção desta norma envia uma mensagem clara aos clientes e às partes interessadas de que a organização dá prioridade à proteção dos seus sistemas e informações.

A norma ISO/IEC 27001:2022 ajuda as organizações a reduzirem a probabilidade de ciberataques, a responderem eficazmente a ataques emergentes, e reduz o risco de perdas e danos na informação através da preparação de pessoas, processos e tecnologias para a gestão de riscos. A norma promove uma abordagem holística da segurança da informação que inclui não só a implementação de controlos técnicos, mas também a gestão de políticas e o envolvimento de todos os níveis da organização.

Esta norma introduz alterações estruturais em relação à versão anterior de 2013. Os controlos do Anexo A da norma, que são a base para os controlos de segurança da informação, foram reorganizados em quatro temas principais, como mostra a Figura 2.2: controlos de pessoas (8 controlos), controlos organizacionais (37 controlos), controlos tecnológicos (34 controlos) e controlos físicos (14 controlos). Esta reorganização facilita a compreensão da forma como estes controlos contribuem para a segurança da informação. Além disso, o número total de controlos diminuiu em relação à versão de 2013, o que reflete uma abordagem mais centrada e simplificada [16].

A ISO/IEC 27001:2022 tem um âmbito relativamente mais reduzido do que a ver-

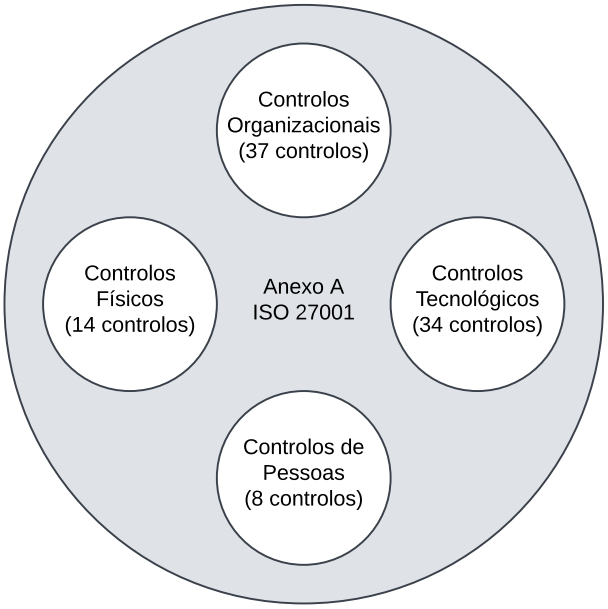

Figura 2.2: *Diagrama do Anexo A da ISO 27001*

são de 2013, uma vez que se centra no alinhamento da norma com outras normas de gestão ISO e na introdução de algumas alterações às cláusulas. Por exemplo, a cláusula 4.2, *Understanding the Needs and Expectations of Interested Parties*, requer agora uma análise detalhada dos requisitos das partes interessadas que serão abordados pelo SGSI, reforçando a compatibilidade com outras normas de gestão. Estas alterações ajudam as organizações a adotar práticas de segurança mais integradas e alinhadas com os requisitos de governação empresarial. Além disso, foram adicionados novos controlos como "A.5.7 *Threat Intelligence*"e "A.5.23 *Information Security for Use of Cloud Services*", que ajudam as organizações a lidar com riscos emergentes e a adotar uma abordagem proativa à cibersegurança. As organizações certificadas pela ISO/IEC 27001:2013 [17] têm até outubro de 2025 para efetuarem a transição para a nova versão.

2.2.2 *National Institute of Standards and Technology* Cybersecurity Framework

A *NIST Cybersecurity Framework* (CSF) 2.0 [18], desenvolvida pelo *National Institute of Standards and Technology* (NIST), é uma *framework* abrangente e flexível que fornece uma metodologia estruturada para ajudar as organizações de todos os setores e dimensões a gerir e mitigar os riscos de cibersegurança.

A CSF 2.0, lançado em fevereiro de 2024, baseia-se na versão anterior, CSF 1.1, que foi introduzida em abril de 2018. Enquanto a CSF 1.1 se concentrava principalmente na gestão de riscos de cibersegurança, a CSF 2.0 expande o seu âmbito para incluir a governação e a gestão de riscos da cadeia de abastecimento. Esta nova versão também enfatiza a melhoria da comunicação entre as partes interessadas e fornece orientações mais detalhadas sobre a implementação [18].

No centro da CSF estão seis funções essenciais, conforme ilustrado na Figura 2.3:

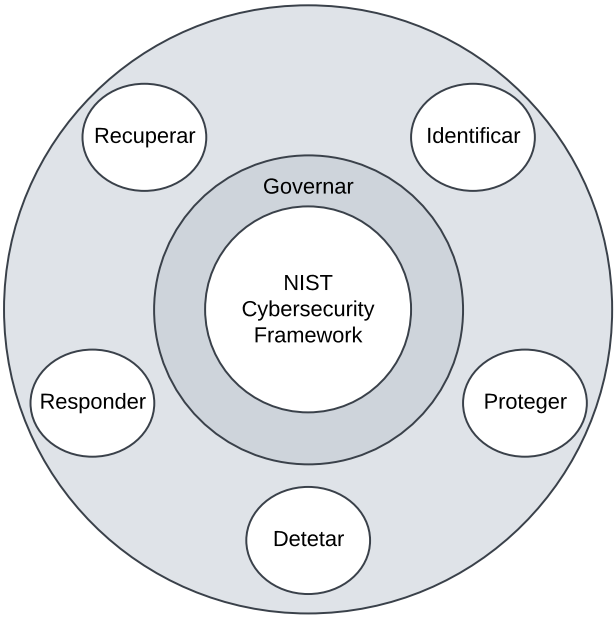

Figura 2.3: *Funções do CSF*

Governar, Identificar, Proteger, Detetar, Responder e Recuperar. Estas funções servem como uma estrutura de alto nível para a gestão dos riscos de cibersegurança e são subdivididas em 22 categorias e 108 subcategorias que detalham resultados e atividades específicas. Um recurso complementar que exemplifica a aplicação prática desta versão é o documento *NIST CSF 2.0 Implementation Examples* [3]. Este guia apresenta exemplos concretos de implementação relacionados com categorias e subcategorias da CSF 2.0. Esta estrutura hierárquica permite às organizações adaptarem as suas estratégias de cibersegurança aos seus perfis de risco e contextos operacionais específicos.

Um dos principais pontos fortes da CSF é a sua capacidade de envolver um público alargado, incluindo executivos, gestores e profissionais técnicos. A utilização de uma linguagem e uma *framework* comum facilita a comunicação sobre os riscos e as estratégias de cibersegurança nos diferentes níveis de uma organização. Esta inclusão é crucial para promover uma cultura de consciencialização e colaboração em matéria de cibersegurança.

A CSF não é prescritivo, em vez disso, fornece uma *framework* flexível que as organizações podem adaptar às suas necessidades específicas. Incentiva a melhoria contínua e o alinhamento com os objetivos comerciais, tornando-o uma ferramenta valiosa para as organizações que procuram melhorar a sua postura de cibersegurança.

2.2.3 CIS *Controls*

Inicialmente, o objetivo principal dos *CIS Critical Security Controls* (CIS *Controls*) [19], desenvolvidos pelo *Center for Internet Security* (CIS), era ajudar indivíduos e organizações a dar o primeiro passo na defesa contra ciberataques. Hoje, no entanto, tornou-se

numa comunidade internacional de pessoas e instituições voluntárias que partilham informações sobre ataques e as suas causas, desenvolvem ferramentas, promovem o alinhamento dos CIS *Controls* com *frameworks* de referência e identificam soluções para problemas e obstáculos.

Os CIS *Controls* são um conjunto de controlos desenvolvidos para mitigar os ciberataques mais comuns e simplificar a adoção de melhores práticas no fortalecimento da postura de segurança cibernética.

A versão 8.1 dos CIS *Controls* fornece mais contexto para cada controlo através de exemplos específicos e explicações adicionais, tornando a sua utilização mais prática. Para além disso, está alinhada, sempre que possível, com outras *frameworks* de segurança relevantes, preservando as características únicas dos CIS *Controls*. Por fim, esta versão garante a consistência dos controlos existentes, assegurando poucas ou nenhumas alterações para os utilizadores atuais [20].

Os CIS *Controls* permitem simplificar a proteção contra ameaças, facilitar a adesão a regulamentos do setor, como o Regulamento Geral sobre a Proteção de Dados (RGPD) [21], e ajudar a alcançar uma boa higiene cibernética. Além disso, ao converterem a informação em ações tangíveis, estes controlos permitem o alinhamento dos requisitos de segurança com os objetivos organizacionais [19].

Nas versões anteriores, os controlos estavam organizados em três categorias: Básicos, Fundamentais e Organizacionais, de modo a refletir diferentes níveis de prioridade e aplicação. Atualmente, existem 18 controlos de nível superior que contribuem para o fortalecimento da postura em cibersegurança.

Os 18 controlos atuais são os seguintes:

1. Inventário e controlo de ativos empresariais;
2. Inventário e controlo de ativos de *software*;
3. Proteção de dados;
4. Configuração segura de ativos empresariais e *software*;
5. Gestão de contas;
6. Gestão de controlo de acessos;
7. Gestão contínua de vulnerabilidades;
8. Gestão de registos de auditoria;
9. Proteções de email e navegador web;
10. Defesas contra *malware*;
11. Recuperação de dados;
12. Gestão de infraestrutura de rede;
13. Monitorização e defesa de rede;
14. Formação em consciencialização e competências de segurança;
15. Gestão de fornecedores de serviços;
16. Segurança do *software* de aplicações;
17. Gestão de resposta a incidentes;
18. Testes de penetração.

Cada controlo é dividido em "*Safeguards*", que são ações específicas a serem implementadas, com o objetivo de apoiar a execução de cada controlo.

2.2.4 *European Cybersecurity Skills Framework*

A *European Cybersecurity Skills Framework* (ECSF) [22] é uma ferramenta útil, desenvolvida pela *European Union Agency for Cybersecurity* (ENISA), que facilita a identificação e organização de tarefas, conhecimentos, aptidões e competências relacionadas com as funções desempenhadas pelos profissionais europeus de cibersegurança. Esta *framework*, é utilizada pela União Europeia (UE) como referência para a definição e avaliação de competências relevantes, em conformidade com a Academia de Competências em Cibersegurança anunciada pela Comissão Europeia. Esta *framework* divide as funções dos profissionais de cibersegurança em 12 perfis [23], como mostra a Figura 2.4, que são normalmente necessários e utilizados pelas organizações que mobilizam peritos em cibersegurança. Estes perfis destacam responsabilidades, competências e habilidades, promovendo um entendimento comum sobre os papéis e conhecimentos necessários, além de apoiar o reconhecimento de competências e o desenvolvimento de programas de formação na área.

Cada perfil é definido por um modelo comum que incorpora critérios-chave estabelecidos, como título, títulos alternativos, resumo, missão, entregáveis, tarefas principais, competências principais, conhecimentos principais e e-Competências (competências necessárias para o uso e gestão de tecnologias digitais). Embora o conteúdo de cada critério seja personalizado para cada função, pode ser modificada para permitir uma implementação flexível que satisfaça necessidades e circunstâncias específicas.

A ECSF baseia-se em vários princípios destinados a responder às exigências das partes interessadas. Isto torna a *framework* simples de compreender, adotar e utilizar, preservando simultaneamente a sua relevância e os seus efeitos a longo prazo. Os princípios que orientam esta *framework* são os seguintes:

- Simples e compreensivo;
- Flexível e escalável;
- Aberto e imparcial.

2.2.5 Quadro Nacional de Referência para a Cibersegurança

O Quadro Nacional de Referência para a Cibersegurança (QNRCS) [24] foi desenvolvido pelo Centro Nacional de Cibersegurança (CNCS) [25]. Pretende apoiar as empresas portuguesas na implementação das bases da cibersegurança, permitindo-lhes cumprir os requisitos mínimos de segurança [26] de redes e sistemas de informação, com o objetivo de reduzir os riscos e os impactos negativos de ataques. Para isto foi criado um documento que fornece uma visão geral do QNRCS e da sua abordagem à gestão dos riscos de cibersegurança. Inclui secções sobre identificação, proteção, deteção, resposta e recuperação de incidentes de segurança (ver Figura 2.5), juntamente

Figura 2.4: *12 perfis do ECSF*
Fonte: ENISA, Role Profiles [23]

com recomendações adicionais para melhorar as práticas organizacionais de cibersegurança, como o papel do *Chief Information Security Officer* (CISO) e a criação de *Security Operations Center* (SOC) e *Computer Security Incident Response Team* (CSIRT).

Para apoiar as organizações, o CNCS complementou o QNRCS com um documento que detalha os três níveis de capacidade (Inicial, Intermédio e Avançado) para cada nível de cibersegurança. Isto permite às organizações avaliar e desenvolver as suas capacidades de acordo com os cinco objetivos de cibersegurança. O nível de capacidade adequado é escolhido com base nas caraterísticas e necessidades únicas de cada organização [24].

O QNRCS estabelece diretrizes específicas para a avaliação da segurança da informação em Portugal, com o objetivo de reforçar a proteção de dados e a resiliência das organizações contra ciberameaças. Estas diretrizes são fundamentais para garantir que as práticas de segurança são eficazes e adaptadas ao contexto nacional. Entre as principais recomendações do QNRCS, destacam-se as seguintes:

1. Avaliação de riscos: As organizações são encorajadas a efetuar avaliações de risco regulares para identificar vulnerabilidades e ameaças específicas às suas operações. Esta abordagem proativa permite às organizações dar prioridade às suas medidas de segurança com base no nível de risco que enfrentam;
2. Planeamento da resposta a incidentes: É crucial que as organizações desenvolvam e mantenham um plano de resposta a incidentes que descreva os procedi-

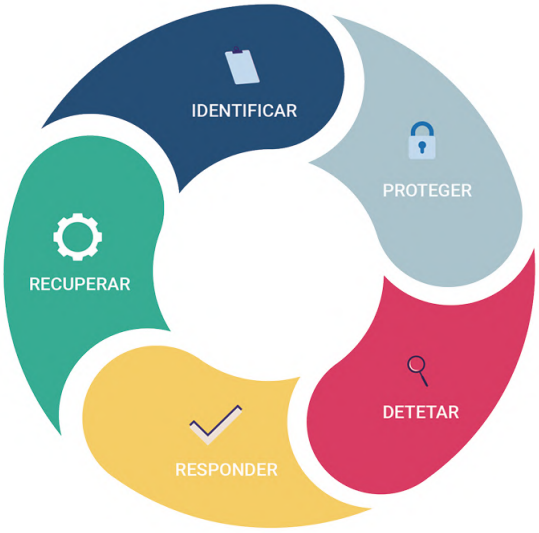

Figura 2.5: *Objetivos de Segurança*
Fonte: CNCS, QNRCS [24]

mentos a seguir no caso de um incidente de cibersegurança. Este plano deve incluir funções e responsabilidades, estratégias de comunicação e processos de recuperação para minimizar o impacto dos incidentes;

3. Formação e sensibilização: Os programas de formação e sensibilização contínuos para os funcionários são essenciais para promover uma cultura de cibersegurança nas organizações. Estes programas devem abranger as melhores práticas, as ameaças potenciais e a importância de aderir às políticas de segurança;
4. Colaboração e partilha de informação: As organizações são encorajadas a colaborar com outras entidades, incluindo os setores públicos e privados, para partilhar informações sobre ameaças e incidentes. Esta colaboração reforça a segurança coletiva e ajuda as organizações a manterem-se informadas sobre os riscos emergentes;
5. Conformidade com os requisitos legais e regulamentares: As organizações devem garantir a conformidade com *frameworks* legais e regulamentares relevantes relacionados com a cibersegurança. Isto inclui a adesão às leis de proteção de dados e regulamentos específicos do setor para mitigar os riscos legais e criar confiança.

A cibersegurança exige competências que abrangem tanto domínios especializados como transversais. Neste contexto, o CNCS elaborou um referencial que identifica as competências e os conhecimentos em matéria de cibersegurança destinado aos participantes do sector e aos empregadores, a fim de facilitar a identificação das competências exigidas nos candidatos. Este referencial tem ainda como objetivo integrar estes temas na estrutura curricular do ensino básico, secundário e superior; apoiar o desenvolvimento profissional contínuo dos professores e promover a formação avançada em cibersegurança no ensino universitário e politécnico.

Este documento organiza as competências em 2 domínios, 6 subdomínios e 36 com-

petências, definidas no documento "Competências e Conhecimentos"[27].

O CNCS elaborou um mapa concetual (Figura 2.6), presente no documento de apresentação do referencial, que explica e desenvolve as relações entre os conceitos de tarefa, função, competência e conhecimento, destacando as interdependências entre esses elementos. Este mapa ajuda a compreender a estrutura lógica do referencial e a forma como as competências se relacionam com as funções e tarefas na área da cibersegurança.

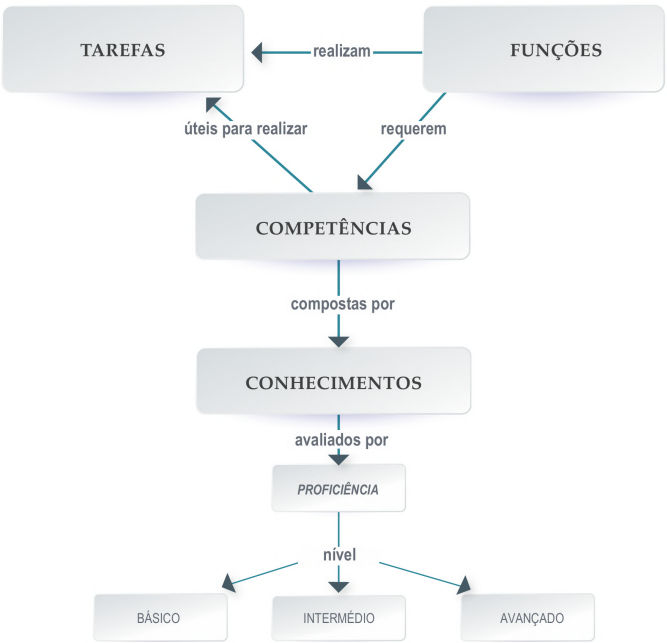

Figura 2.6: *Mapa Conceptual*
Fonte: CNCS, Referencial [24]

2.3 Frameworks Relevantes para Auditorias de Segurança

As auditorias de segurança são componentes essenciais na avaliação e fortalecimento das práticas de cibersegurança em organizações de todos os tamanhos e setores. Para garantir auditorias eficazes e a conformidade com as normas internacionais, foram desenvolvidas várias *frameworks* para orientar os profissionais da área na identificação de riscos, avaliação de vulnerabilidades e implementação de medidas de mitigação. Nesta secção, são analisadas algumas das principais *frameworks* relevantes para auditorias de segurança, como a NIST SP 800-115, a ISO/IEC 27007:2020, o CSAM e o CIS RAM, destacando a sua aplicabilidade, objetivos e impacto na melhoria da postura de segurança das organizações.

2.3.1 NIST SP 800-115

A Publicação Especial NIST 800-115 [8], desenvolvida pelo *National Institute of Standards and Technology* (NIST) em 2008 e intitulada "Technical Guide to Information Se-

curity Testing and Assessment", foi criada para responder à necessidade crescente das organizações avaliarem a sua postura de segurança e identificarem fraquezas nos seus sistemas, à medida que as tecnologias da informação se tornam fundamentais para as operações empresariais. O guia fornece orientações abrangentes sobre como realizar avaliações de segurança em sistemas de informação, com base em melhores práticas e experiências do mundo real. Ao combinar princípios teóricos com estratégias acionáveis, o NIST SP 800-115 apresenta metodologias práticas e uma *framework* estruturada para ajudar as organizações a enfrentarem os desafios de segurança e a garantir a Confidencialidade, Integridade e Disponibilidade (CIA) dos seus sistemas de informação. Ele foca-se em técnicas práticas para avaliar controlos de segurança, identificar vulnerabilidades e avaliar a eficácia da estratégia de segurança da organização.

O NIST SP 800-115 é altamente relevante para auditorias de segurança porque fornece diretrizes estruturadas sobre como avaliar as medidas de segurança de forma eficaz e oferece uma *framework* para os auditores seguirem que garante que as auditorias são abrangentes e cobrem todos os aspetos necessários da segurança da informação, desde a identificação de ativos e riscos, até à realização de testes aos controlos de segurança. A publicação enfatiza a importância da validação prática, como testes de penetração, *scans* de vulnerabilidades e revisões de configurações, que são componentes essenciais de qualquer auditoria de segurança.

A implementação do NIST 800-115 pode ser desafiadora, dependendo do tamanho, complexidade e maturidade do programa de segurança da organização. Empresas pequenas podem achar mais fácil implementá-lo, enquanto empresas maiores, com sistemas mais complexos, podem precisar de mais recursos e experiência para adotar completamente a *framework*. No entanto, as orientações fornecidas pelo NIST 800-115 podem simplificar o processo, especialmente quando combinada com ferramentas automatizadas e equipas especializadas em segurança. É importante notar que a implementação eficaz requer uma compreensão sólida das técnicas de testes de segurança, bem como a capacidade de analisar e responder adequadamente às descobertas.

O NIST 800-115 pode ser utilizado por uma variedade de organizações e profissionais envolvidos na segurança da informação, incluindo:

- Auditores de segurança de TI e *pentesters* que necessitam de uma abordagem estruturada para avaliar e testar sistemas;
- Consultores de cibersegurança que aconselham clientes sobre como melhorar a sua postura de segurança;
- Responsáveis pela conformidade que garantem que as organizações cumprem os requisitos regulamentares relacionados com a segurança da informação;
- Equipas de segurança internas das organizações, particularmente aquelas encarregues de realizar avaliações de segurança regulares e manter as melhores práticas de segurança.

Devido à sua ampla aplicabilidade, o NIST 800-115 pode ser utilizado por organizações do setor público e privado, independentemente do tamanho ou setor.

2.3.2 ISO/IEC 27007:2020

A norma ISO/IEC 27007:2020 [15] fornece diretrizes para a realização de auditorias de Sistema de Gestão da Segurança da Informação (SGSI) para garantir a conformidade com a norma ISO/IEC 27001. A norma oferece orientações pormenorizadas sobre o planeamento, a realização e a comunicação de auditorias de SGSI, abrangendo elementos-chave como a seleção de critérios de auditoria adequados, como os requisitos da ISO/IEC 27001, práticas de gestão de riscos de segurança, conformidade regulatória, melhores práticas do setor e a formulação de recomendações de melhorias.

Com o aumento da pressão sobre as organizações para gerir e proteger grandes volumes de dados, especialmente informações sensíveis, a implementação de práticas de segurança robustas torna-se fundamental. Violações de dados que envolvem o roubo de informações pessoais sensíveis, financeiras ou médicas demonstraram que uma segurança de dados inadequada pode ter consequências graves, desde perdas financeiras a danos na reputação [28]. Neste contexto, a norma ISO/IEC 27007 desempenha um papel fundamental ao oferecer uma abordagem estruturada para auditar o SGSI, assegurando que as organizações estão a proteger os seus ativos de informação de forma eficaz.

Com o aumento da atenção dada à proteção de dados, especialmente com regulamentos como o RGPD, as organizações precisam não só de cumprir os requisitos legais, mas também de garantir às partes interessadas, incluindo clientes e parceiros, que as suas informações estão seguras. A ISO/IEC 27007 ajuda as organizações a satisfazerem estas expetativas, fornecendo uma estrutura clara para avaliar a eficácia do seu SGSI, garantindo que as medidas de segurança estão alinhadas com as normas internacionais e que as potenciais lacunas ou fraquezas são identificadas e resolvidas.

A ISO/IEC 27007 oferece uma estrutura de auditoria abrangente que cobre vários aspetos de um SGSI, incluindo [29]:

- Conformidade com a ISO/IEC 27001: A norma garante que as organizações cumprem os requisitos essenciais da ISO/IEC 27001, que se centra na gestão dos riscos de segurança da informação e no estabelecimento de um SGSI eficiente;
- Requisitos das partes interessadas: Incorpora as diretrizes e os requisitos definidos pelas partes interessadas, tais como parceiros comerciais, clientes e entidades reguladoras, garantindo que a auditoria aborda necessidades e expectativas específicas;
- Obrigações regulamentares e estatutárias: A norma ajuda as organizações a cumprir as suas responsabilidades legais e regulamentares relativamente à segurança e privacidade dos dados. Ao fazê-lo, ajuda as organizações a manter a conformidade com as leis de proteção de dados e a evitar sanções;
- Processos e controlos do SGSI: A ISO/IEC 27007 fornece uma análise detalhada dos processos, controlos e objetivos de segurança do SGSI de uma organização. Isto ajuda os auditores a avaliar se o sistema está a funcionar como pretendido e se está a cumprir os objetivos de segurança.

O âmbito da ISO/IEC 27007 permite que seja adaptada às necessidades específicas de cada organização, independentemente da sua dimensão, o que a torna adequada para uma variedade de situações de auditoria, desde grandes equipas que realizam auditorias em grandes empresas, a equipas mais pequenas ou auditores individuais que trabalham em empresas mais pequenas. A ISO/IEC 27007 pode ser utilizada para auditorias internas na organização, bem como para auditorias em que estão envolvidos fornecedores de serviços externos.

Além disso, a norma ISO/IEC 27007:2020 sublinha a importância de estabelecer objetivos claros para o programa de auditoria (cláusula 5.2.2). Estes objetivos incluem a demonstração da conformidade com os requisitos legais e contratuais, a avaliação da eficácia das medidas de gestão dos riscos e a promoção da confiança na capacidade da organização para gerir eficazmente os riscos de segurança. A norma está alinhada com a ISO 19011:2018 [30] e inclui princípios como a integridade, a apresentação justa das conclusões e resultados da auditoria, e uma abordagem baseada no risco para garantir que as auditorias são sistemáticas e fiáveis (cláusula 4 da norma).

A competência do auditor é um ponto-chave (cláusula 7), com a norma a sublinhar a necessidade de conhecimentos especializados em segurança da informação, assim como de manter e aprimorar continuamente essa competência. O Apêndice A da ISO/IEC 27007:2020 fornece orientações práticas sobre a auditoria dos processos do SGSI, incluindo a utilização de provas como entrevistas, análises de documentos e observações. Estas práticas foram pensadas para estabelecer uma ligação entre as conclusões da auditoria aos objetivos e controles do SGSI da organização, tornando o processo de auditoria mais eficaz.

2.3.3 *The CyberSecurity Audit Model*

O *CyberSecurity Audit Model* (CSAM) [31, 32] é uma *framework* abrangente e adaptável, concebida para a realização de auditorias de cibersegurança em organizações de qualquer dimensão ou setor, assim como para a avaliação de estratégias de cibersegurança a nível nacional. Inicialmente introduzido em 2017, o modelo CSAM 1.0 [31] foi posteriormente expandido e atualizado, culminando na versão CSAM 2.0 [32] em 2023, que aborda de forma mais abrangente e diversificada os desafios de cibersegurança.

O CSAM 1.0 foi desenvolvido como uma solução para a realização de auditorias detalhadas de cibersegurança em organizações ou países que avaliam a sua *National Cybersecurity Strategy* (NCS). A sua estrutura assentava em 18 domínios de cibersegurança, suportados por 87 *checklists*, 169 controlos, 429 sub-controlos e num sistema de avaliação de desempenho. Esta *framework* oferece uma abordagem flexível, permitindo aos auditores realizar auditorias parciais centradas em domínios específicos, ou efetuar uma auditoria completa para avaliar todas as áreas de cibersegurança de uma organização. O modelo tinha como objetivo principal:

- Avaliar a preparação e a maturidade da cibersegurança;
- Fornecer diretrizes para melhorar a postura de cibersegurança;

- Permitir auditorias parciais ou completas em domínios específicos.

A versão atualizada, CSAM 2.0, lançada em junho de 2023, introduziu melhorias, como:

- Expansão para 30 domínios: Foram incorporados domínios como segurança na *cloud*, testes de penetração e as auditorias do SOC, o que permite ao CSAM 2.0 cobrir um cenário de segurança cibernética mais amplo;
- Sistemas de controlo industrial e de fabrico: O âmbito inclui agora auditorias para sistemas de controlo industrial e de fabrico;
- Segurança do fornecedor e da cadeia de fornecimento: Dada a crescente relevância da segurança na cadeia de fornecimento, foram incorporadas novas capacidades de auditoria específicas para esse fim;
- Capacidades de auditoria avançadas: Inclui 99 *checklists*, 225 controlos e 549 subcontrolos, tornando as avaliações mais rigorosas e adaptáveis;
- Educação e formação em cibersegurança: Esta versão introduziu avaliações para programas de educação, *CyberSecurity Education, Training, and Awareness* (CSETA) dentro das organizações.

Uma das novidades na CSAM 2.0 é a inclusão de diretrizes para a avaliação de estratégias e políticas nacionais de cibersegurança. Isto permite uma abordagem mais holística, não só centrada na segurança organizacional, mas também na preparação para a cibersegurança no contexto nacional. Isto torna a CSAM 2.0 particularmente relevante para auditorias a nível nacional, onde fornece uma *framework* para avaliar as políticas nacionais de cibersegurança e a sua implementação.

Além disso, o CSAM 2.0 inclui uma *framework* de pontuação de maturidade que quantifica a eficácia da cibersegurança em todas as áreas auditadas, que ajuda as organizações a direcionarem os seus recursos para as áreas mais críticas de segurança. Cada domínio auditado é classificado numa escala de 1 a 500, correspondendo ao nível de implementação e eficácia das práticas de segurança nesse domínio, conforme detalhado a seguir:

- **Inexistente (I): 0**
  Falta de capacidades de cibersegurança.
- **Imaturo (Im): 1-125**
  A organização não tem quaisquer planos para gerir a sua cibersegurança. Os controlos das áreas críticas de cibersegurança são inexistentes ou muito fracos. A organização não implementou um programa abrangente de cibersegurança.
- **Em desenvolvimento (D): 126-250**
  A organização está a começar a concentrar-se em questões de cibersegurança. Se as tecnologias estiverem implementadas, a organização precisa de se concentrar em áreas-chave para proteger os ativos cibernéticos. A atenção deve centrar-se no pessoal, nos processos, nos controlos e nos regulamentos.

- **Maduro (M): 251-375**
  Embora a organização tenha um ambiente maduro, são necessárias melhorias nas áreas-chave que foram identificadas com pontos fracos.
- **Avançado (A): 376-500**
  A organização tem-se destacado na implementação das melhores práticas de cibersegurança. Há sempre espaço para melhorias. Deve manter a documentação atualizada e realizar revisões regulares dos processos de cibersegurança por meio de auditorias contínuas.

O nível final de maturidade é obtido pela média das pontuações de todos os domínios auditados, o que permite classificar a maturidade geral de cibersegurança.

2.3.4 *CIS Risk Assessment Method*

O *CIS Risk Assessment Method* associa os ativos de informação às salvaguardas do CIS que os protegem. Este processo também inclui a identificação das vulnerabilidades que podem estar presentes nos ativos e das ameaças que podem comprometer a sua segurança. Esta abordagem é delineada no *Risk Assessment Method* (RAM) [33], que salienta a necessidade de uma análise exaustiva dos riscos. Este processo é particularmente relevante para as auditorias de segurança, uma vez que estabelece claramente as ligações entre os ativos de informação, as salvaguardas e as ameaças, permitindo avaliar o impacto nos objetivos da empresa e dar prioridade às ações destinadas a atenuar os riscos identificados.

A seguir, descreve-se como o método é aplicado na prática durante a avaliação de riscos:

1. Modelação dos riscos: O primeiro passo consiste em identificar o ativo de informação ou a classe de ativos em avaliação, que pode incluir dispositivos específicos, como *firewalls*, aplicações ou conjuntos de servidores. A etapa seguinte consiste em identificar as ameaças que podem comprometer a Confidencialidade, Integridade e Disponibilidade (CIA) desses ativos. O avaliador de riscos enumera então as salvaguardas CIS relevantes para proteger estes ativos contra as ameaças identificadas. As vulnerabilidades também são consideradas, incluindo potenciais falhas na implementação das salvaguardas, tais como erros administrativos, falhas de sistema ou recursos insuficientes;
2. Critérios para a análise do risco: O avaliador de riscos documenta os elementos-chave de uma análise de riscos, incluindo a salvaguarda do CIS, o ativo de informação, a ameaça identificada, a implementação da salvaguarda e as vulnerabilidades. Estimar o impacto e a expetativa dos riscos é crucial nesta fase, embora possa ser um desafio. Para ajudar neste processo, o CIS RAM fornece definições para estimar estes valores. Os níveis de risco são avaliados com base em critérios predefinidos que classificam os riscos como negligenciáveis, aceitáveis, elevados ou catastróficos, como ilustrado na Figura 2.7;

Definition:	Define the enterprise's Mission (why the risk is worth engaging):	Define the enterprise's Operational Objectives (the enterprise's goals):	Define the enterprise's Obligations (duty of care owed to others):
1 **Negligible**	Describe a negligible impact to the Mission.	Describe a negligible impact to the Operational Objectives.	Describe a negligible impact to the Obligations.
2 **Acceptable**	Describe an acceptable impact to the Mission.	Describe an acceptable impact to the Operational Objectives.	Describe an acceptable impact to the Obligations.
3 **Unacceptable**	Describe an unacceptable impact to the Mission.	Describe an unacceptable impact to the Operational Objectives.	Describe an unacceptable impact to the Obligations.
4 **High**	Describe a high, recoverable impact to the Mission.	Describe a high, recoverable impact to the Operational Objectives.	Describe a high, recoverable impact to the Obligations.
5 **Catastrophic**	Describe an unrecoverable impact to the Mission.	Describe an unrecoverable impact to the Operational Objectives.	Describe an unrecoverable impact to the Obligations.

Figura 2.7: *Critérios de impacto diretrizes de definição*
Fonte: CIS, CIS RAM v2.1 [33]

3. Recomendação de salvaguardas do CIS: Uma vez identificados os riscos, estes devem ser tratados através do reforço das salvaguardas existentes ou da implementação de novas medidas de mitigação. Se o risco for aceite, significa que a organização determinou que se encontra dentro dos limites aceitáveis e que não são necessárias ações imediatas, embora a monitorização contínua seja essencial para garantir que se mantém aceitável. Para os riscos que não podem ser aceites, devem ser implementadas medidas adicionais, como a formação dos funcionários ou a implementação de *firewalls* de rede, para reduzir o risco para um nível aceitável. Esta decisão é documentada juntamente com os detalhes da salvaguarda, incluindo a sua pontuação de maturidade, a eficácia esperada, o impacto na missão e nos objetivos operacionais e custos associados. É importante avaliar cuidadosamente estas salvaguardas para garantir que reduzem o risco sem introduzir riscos novos e inaceitáveis;
4. Avaliação das salvaguardas recomendadas: Ao recomendar novas medidas de segurança, os avaliadores de risco devem considerar que, embora estas possam reduzir os riscos numa área, podem também aumentar os riscos noutras. Este duplo efeito é a razão pela qual o CIS RAM introduz o conceito de "Risco de Salvaguarda". Por exemplo, salvaguardas como controlos de acesso rigorosos podem diminuir a produtividade ou incentivar soluções alternativas pouco seguras. Por conseguinte, todas as salvaguardas devem ser cuidadosamente implementadas para garantir que cumprem o objetivo de redução do risco sem criar inadvertidamente novos riscos mais elevados;
5. Aceitabilidade do risco da salvaguarda: É fundamental avaliar se as novas salvaguardas criam riscos superiores aos que se destinam a mitigar. Se a pontuação de risco de uma salvaguarda for inferior ao risco original, é normalmente considerada um tratamento eficaz. No entanto, deve ser considerada uma alternativa para atenuar o impacto se a classificação do risco de uma salvaguarda for mais elevada do que o risco original.

3
Trabalhos Relacionados

Este capítulo explora uma seleção de estudos e *frameworks* relevantes que abordam desafios e soluções em cibersegurança, com foco especial nas Pequenas e Médias Empresas (PME) e nas diferentes abordagens para a implementação de normas internacionais, como a ISO/IEC 27001 e o NIST CSF. Os trabalhos discutidos aqui fornecem uma visão abrangente das dificuldades enfrentadas pelas PMEs em matéria de segurança cibernética, as metodologias de avaliação de riscos adotadas, e as boas práticas que emergem da implementação de *frameworks* de segurança em diferentes contextos organizacionais e geográficos.

3.1 *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*

Neste trabalho [34], os autores destacam que as Pequenas e Médias Empresas (PME) enfrentam grandes dificuldades para alcançarem um nível adequado de resiliência face a ciberameaças, muitas vezes devido à falta de conhecimento, recursos financeiros insuficientes e pouca formação sobre os riscos de cibersegurança. Dos 916 estudos analisados pelos autores, 77 foram identificados como relevantes, tendo surgido 44 temas únicos. No entanto, a maioria dos temas abordados carecia de profundidade, indicando uma evolução limitada da investigação sobre a cibersegurança das PME.

Os principais desafios para as PME incluem uma consciência limitada dos riscos de cibersegurança, recursos financeiros limitados e uma literacia em cibersegurança reduzida, que é particularmente acentuada nos países em desenvolvimento. Uma constatação recorrente é que a baixa literacia em cibersegurança agrava os desafios da sensibilização e do financiamento. Este facto realça a necessidade de iniciativas educativas específicas para melhorar a compreensão da cibersegurança por parte das PME e permitir a tomada de decisões informadas.

Muitas PME não têm uma liderança sólida em matéria de cibersegurança, o que as deixa sobrecarregadas ou a funcionar com medidas de segurança mínimas. Apesar

destes desafios, algumas conclusões destacam desenvolvimentos positivos. Por exemplo, a adoção de soluções em *cloud* mostrou ter potencial para reduzir alguns desafios de cibersegurança e uma maior conscientização sobre os riscos levou à adoção de práticas de cibersegurança mais eficazes.

3.2 *On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations*

No estudo [35] realizado, as organizações portuguesas enfrentam várias dificuldades na implementação e certificação da ISO/IEC 27001:2013 [17], uma norma destinada a apoiar a gestão da segurança da informação. A investigação destacou vários obstáculos, sendo o principal desafio o custo financeiro da implementação. Muitas organizações gastaram mais de 50 000 euros, incluindo salários de funcionários, investimentos em infra-estruturas de segurança e consultoria externa. Para as organizações com orçamentos mais limitados, este foi um obstáculo significativo.

Além disso, 24% das organizações tiveram dificuldades em definir o âmbito da implementação, enquanto 68% tiveram dificuldades em interpretar a norma e a sua documentação. A resistência à mudança também foi evidente, com 28% das organizações a depararem-se com desafios na adaptação a novos processos. Uma questão fundamental foi a dificuldade em atribuir funções e responsabilidades, uma vez que 72% das organizações tiveram contratempos nesta área.

Outra dificuldade foi a longa duração do processo de implementação, que exigiu esforços substanciais para alinhar políticas, atribuir recursos e integrar controlos de segurança nas operações comerciais. Algumas organizações também enfrentaram problemas com a definição de políticas de segurança claras e com a garantia de conformidade entre departamentos. Além disso, a maioria das organizações (mais de 90%) não tinham políticas de segurança em vigor antes de iniciar o processo de certificação.

Apesar destes desafios, as organizações que implementaram com sucesso a ISO/IEC 27001:2013 registaram melhorias na conformidade, na confiança dos clientes e na eficiência operacional. O processo de certificação resultou numa abordagem mais estruturada à gestão dos riscos de segurança, tornando as organizações mais adaptáveis às mudanças e mais bem preparadas para lidar com incidentes de cibersegurança. Além disso, as organizações descobriram que a certificação ISO/IEC 27001 facilitou a conformidade com os requisitos do RGPD, garantindo a proteção e a privacidade dos dados.

3.3 *Enhancing Cybersecurity for SMEs: A Structured Framework for IT Security Assessment*

Este documento [36] apresenta uma *framework* modular de avaliação de segurança de TI para PMEs que aborda os desafios de cibersegurança que estas enfrentam devido a recursos e conhecimentos limitados. Com a evolução das tecnologias digitais, as

PME têm acesso a novas oportunidades de crescimento, mas também se deparam com desafios significativos de segurança. A *framework* proposta simplifica este processo com três módulos principais: Avaliação Operacional, Avaliação de Segurança e Avaliação do Pessoal.

A avaliação operacional avalia se a infraestrutura de TI de uma PME suporta as suas necessidades comerciais. Considera a eficiência do *hardware*, *software* e redes, bem como os processos utilizados para os gerir e monitorizar, garantindo uma cobertura abrangente do desempenho operacional.

A avaliação da segurança centra-se nas vulnerabilidades, abrangendo as atualizações de *software*, as vulnerabilidades conhecidas, a segurança da rede e a proteção dos ativos. Além disso, propõe estratégias práticas de mitigação, reconhecendo as limitações de recursos das PMEs que podem dificultar uma resposta corretiva imediata.

A avaliação dos recursos humanos avalia o aspeto humano da cibersegurança, incluindo as qualificações dos funcionários, a sensibilização para a segurança e a adesão aos protocolos. Inclui avaliações práticas, como simulações, para testar as respostas dos funcionários às ameaças à segurança e avaliar a eficácia da formação.

A natureza modular da *framework* permite que as PME adaptem a avaliação às suas necessidades específicas, dando prioridade a áreas que se alinham com os seus objetivos de negócio e recursos disponíveis. Ao adotar uma abordagem de avaliação orientada para a solução, que combina a deteção de vulnerabilidades com a mitigação de riscos, a *framework* ajuda as PME não só a identificar os pontos fracos, mas também a adotar uma postura mais proativa na gestão dos riscos de cibersegurança. Esta abordagem melhora a postura geral de segurança das PMEs, permitindo-lhes tirar partido das ferramentas e inovações digitais, minimizando simultaneamente a sua exposição a ciberameaças em evolução.

3.4 *Adaptable Security Maturity Assessment and Standardization for Digital SMEs*

O autor [37] argumenta que as PME são fundamentais para a economia, mas enfrentam grandes desafios em matéria de cibersegurança devido a recursos limitados. Os modelos de maturidade existentes ignoram frequentemente as necessidades específicas e o papel das PME no ecossistema digital. Para resolver este problema, a *framework* ASMAS fornece uma abordagem adaptada à avaliação e normalização da maturidade da cibersegurança.

A Aliança Europeia para as PME Digitais propõe diversas categorias de PME: facilitadores digitais, digitalmente baseadas, digitalmente dependentes e empresas em fase de arranque. Partindo destas categorias, a *framework* alinha as capacidades de segurança com os perfis organizacionais [38]. Por exemplo, as empresas em fase de arranque, que muitas vezes não têm consciência das necessidades de cibersegurança, são avaliadas em relação a um conjunto reduzido de 79 capacidades, enquanto as PME di-

gitalmente dependentes são avaliadas em relação a 115 das 251 capacidades propostas pela *framework*.

As capacidades são derivadas de normas como a NIST *Cybersecurity Framework* e são organizadas em níveis de A a D para simplificar a implementação, sendo o nível A de implementação obrigatória, seguido pelas capacidades dos níveis B, C e D. As PME avaliam o seu progresso utilizando estados de implementação como "totalmente implementado" ou "parcialmente implementado", e os resultados podem ser visualizados em gráficos circulares.

Ao adaptar-se aos requisitos únicos e às restrições operacionais das PME, a *framework* ASMAS garante melhorias práticas e incrementais na cibersegurança.

3.5 *NIST SP 800-115 Framework Implementation using Black Box Method on Security Gaps Testing on JTD Polinema's Official Website*

Os autores deste trabalho [39] aplicaram a *framework* NIST SP 800-115 [8] num cenário de teste de penetração de caixa negra, em que o auditor não tinha conhecimento prévio do sistema alvo. O processo seguiu as quatro fases principais descritas na *framework*: planeamento, descoberta, ataque e elaboração de relatórios.

Planeamento: Durante esta fase, o autor definiu o âmbito do teste de penetração, identificou os objetivos do teste e selecionou as ferramentas adequadas. O planeamento envolveu a determinação dos sistemas e aplicações a testar, bem como os métodos e técnicas que seriam utilizados.

Descoberta: Esta fase foi dividida em duas etapas principais: recolha de informações e análise de vulnerabilidades.

- Recolha de informações: O autor utilizou ferramentas como ping [40], whois [41] e Nmap [42] do Kali Linux [43] para recolher dados sobre o sistema alvo. Esta etapa forneceu informações tais como endereços IP e portas abertas, que formaram a base para a análise de vulnerabilidade subsequente;
- Análise de vulnerabilidade: Após a recolha de informações, o autor usou o OWASP ZAP [44] para analisar as vulnerabilidades do sistema alvo. As descobertas foram categorizadas em diferentes níveis de gravidade, nomeadamente de alta prioridade, média prioridade, baixa prioridade e de informação. Esta classificação ajudou a priorizar as vulnerabilidades para testes adicionais.

Ataque: Com base nos resultados da fase de descoberta, o autor efetuou ataques às vulnerabilidades identificadas. Esta fase centrou-se na tentativa de explorar as falhas de segurança para determinar o risco e o potencial impacto nos sistemas alvo. Os testes foram executados de acordo com cenários predefinidos derivados da análise anterior.

Relatórios: Após a fase de ataque, o autor documentou os resultados, resumindo o sucesso ou o fracasso das tentativas de penetração. O relatório também fornece uma

análise detalhada das vulnerabilidades, descrevendo os riscos potenciais e as etapas seguidas ao longo do processo de teste.

3.6 *Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law*

O documento [45] descreve uma abordagem metodológica que combina o NIST e a ISO para responder às necessidades de auditoria de cibersegurança e avaliação de riscos em Camarões. A metodologia está estruturada em torno de um modelo hierárquico, centrado no nível nacional, nos processos críticos do país e nos sistemas de informação.

Ao nível nacional, a abordagem centra-se no alinhamento das estratégias de gestão do risco com a missão e os objetivos do país. Integra as diretrizes do NIST e da ISO para melhorar a gestão estratégica da segurança da informação através de políticas, procedimentos e mecanismos operacionais. A ISO desempenha um papel importante neste contexto devido à sua *framework* estruturada para a gestão dos SGSI.

Para os processos críticos, a metodologia concentra-se na avaliação dos riscos específicos de cada área funcional e na adaptação das estratégias de gestão do risco de forma adequada. A metodologia combina controlos da ISO e do NIST para garantir a proteção dos ativos e a segurança das operações essenciais, equilibrando os requisitos estratégicos com as considerações técnicas para os processos do país.

Ao nível dos sistemas de informação, a metodologia dá ênfase a avaliações técnicas, como testes de penetração e análise de vulnerabilidades, para identificar e mitigar riscos específicos do sistema. O NIST desempenha um papel proeminente, particularmente o NIST 800-53, que oferece controlos de segurança detalhados e específicos. A aplicação do NIST destaca a sua eficácia na resolução de desafios técnicos, incluindo os relacionados com tecnologias emergentes como a computação em nuvem. Quando combinada com as políticas mais amplas da ISO, a abordagem garante uma cobertura abrangente dos requisitos técnicos e estratégicos.

O NIST 800-53 e a ISO 27001 servem como referências principais para orientar as avaliações e auditorias de risco. Os controlos técnicos detalhados do NIST são particularmente úteis para enfrentar desafios específicos de cibersegurança, enquanto os processos estruturados da ISO melhoram a gestão estratégica a todos os níveis.

Em resumo, a metodologia adota a abordagem estruturada da ISO e recorre ao NIST para o controlo técnico nos sistemas de informação, combinando ambos para responder de forma eficaz às necessidades técnicas e estratégicas.

3.7 *Cybersecurity Framework for SMEs in Peru Based on ISO/IEC 27001 and CSF NIST Controls*

Neste documento [46] foi desenvolvida uma *framework* de cibersegurança para PMEs no Peru, com base nos controlos ISO/IEC 27001 e NIST CSF. Destaca uma abordagem

"harmonizada" que aproveita os pontos fortes de ambas as normas. Este processo de harmonização envolve a seleção e integração de controlos complementares das duas frameworks para responder eficazmente às necessidades específicas das PMEs.

Para esta *framework*, os controlos NIST CSF foram categorizados em quatro funções: identificar, proteger, responder e recuperar com 18 controlos específicos escolhidos. Simultaneamente, a ISO/IEC 27001 contribuiu com controlos de 12 domínios, e foram selecionados 28 controlos para se alinharem com os objetivos da *framework*. O processo de seleção foi orientado pela técnica de avaliação de peritos, que incluiu o contributo de especialistas em cibersegurança para garantir que os controlos são relevantes e práticos para as PME no Peru.

3.8 *A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard*

Este documento [47] compara o NIST CSF e a ISO 27001, e destaca a sua adequação a diferentes tipos de organizações. Ambas fornecem diretrizes para estabelecer um SGSI, mas respondem a necessidades diferentes. O NIST CSF é mais adequado para empresas centradas em tecnologia, uma vez que dá ênfase aos controlos técnicos, análise de registos e gestão de incidentes, enquanto a ISO 27001 é mais apropriada para empresas comerciais.

A principal vantagem do NIST CSF reside no seu formato estruturado e de fácil utilização, que simplifica a implementação numa organização. O seu alinhamento com outras normas, como a ISO 27001 e o COBIT [11], torna-a mais flexível, permitindo a integração com várias abordagens de segurança, como os controlos CIS para a defesa em profundidade. Por outro lado, o reconhecimento global da ISO 27001 faz dela a escolha preferida das organizações que procuram uma norma robusta para ganhar confiança das partes interessadas. Outra vantagem da ISO 27001 é a ênfase extremamente rigorosa e estruturada que coloca na documentação, tanto obrigatória como não obrigatória.

Em última análise, em vez de escolher uma em detrimento da outra, o documento conclui que a combinação dos pontos fortes de ambas as estruturas oferece a abordagem mais eficaz para a criação de um sistema de gestão da cibersegurança resiliente e abrangente.

3.9 *Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security*

No estudo [48] realizado, a ISO/IEC 27001 e o NIST CSF partilham um foco consistente e holístico na segurança da informação, que aborda a segurança das TI, os processos organizacionais e os fatores humanos. Ambas enfatizam a modularidade e a flexibilidade, permitindo implementações personalizadas para organizações de diferentes tamanhos e recursos. A ISO/IEC 27001 adota uma abordagem orientada para os processos, dando ênfase à documentação e ao ciclo *Plan–Do–Check–Act* (PDCA) [49] para gerir um SGSI. Em contraste, o NIST CSF adopta uma metodologia orientada para o risco para identificar e dar prioridade às lacunas de segurança. Enquanto a ISO/IEC 27001 está alinhada com a sua própria família de normas, o NIST CSF incorpora uma gama mais alargada de referências, permitindo a compatibilidade entre os dois métodos para melhorar a segurança organizacional.

3.10 *Cybersecurity and Risk Management Framework in Avionics*

O documento [50] demonstra como as *frameworks* do NIST, especificamente o SP 800-53 [9] e o SP 800-171 [51], foram implementadas no desenvolvimento de aviónica para cumprir os requisitos de cibersegurança para aplicações do *Department of Defense* (DoD). A abordagem incorpora o *Risk Management Framework* (RMF) como base para abordar sistematicamente os riscos. Os requisitos de segurança são capturados e geridos utilizando ferramentas como o DOORS [52] e o eMASS [53].

A integração dos controlos NIST é facilitada pela utilização de uma *Security Requirements Traceability Matrix* (SRTM), que assegura um mapeamento claro entre os controlos prescritos e os componentes do sistema. Este processo não só alinha os controlos técnicos e políticos, como também integra as atividades de verificação e validação (V&V) diretamente no ciclo de vida do desenvolvimento. Ao incorporar estas práticas, o processo de desenvolvimento aborda as questões de Confidencialidade, Integridade e Disponibilidade (CIA), mantendo o alinhamento com as normas de segurança do DoD.

Esta implementação demonstra um método estruturado para integrar as *frameworks* do NIST no processo de desenvolvimento e demonstra a sua relevância e adaptabilidade para cumprir requisitos rigorosos de cibersegurança em domínios altamente regulamentados.

3.11 Síntese dos Desafios de Cibersegurança para PMEs

A análise dos trabalhos relevantes mostra que as PME enfrentam desafios significativos na aplicação de práticas eficazes de cibersegurança, principalmente devido à falta de recursos e de conhecimentos especializados. Muitos destes estudos abordam a necessidade de *frameworks* adaptadas, que salientam a importância de uma abordagem de auditoria adaptada a este tipo de organização. Além disso, a integração de metodologias como a NIST, a ISO/IEC e outros controlos de segurança foi identificada como fundamental para criar uma resiliência em cibersegurança sólida.

4
Metodologia

Neste capítulo é detalhada a metodologia desenvolvida, abordando, por um lado, a abordagem geral adotada no desenvolvimento deste projeto, e, por outro, a metodologia específica seguida para a construção do roteiro de auditoria.

A metodologia deste relatório, conforme ilustrado na Figura 4.1, é dividida em três fases distintas: Fase 1 – Investigação, Fase 2 – Desenvolvimento e Fase 3 – Validação.

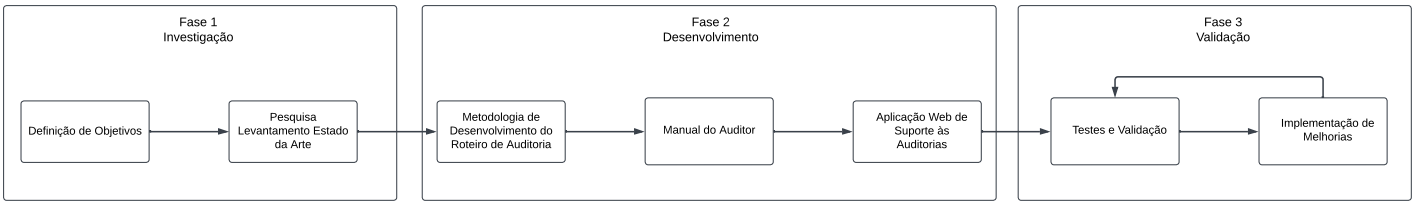

Figura 4.1: *Descrição global da metodologia*

4.1 Fase 1 - Investigação

A fase inicial deste processo envolve a definição dos objetivos e a pesquisa do estado da arte, com o objetivo de estruturar o desenvolvimento da auditoria de forma clara e objetiva, garantindo uma base sólida para as fases subsequentes.

4.1.1 Definição de Objetivos

Na primeira fase, foram definidos os objetivos deste trabalho: 1) criar um roteiro de auditoria; 2) criar um manual de auditor e 3) validar estes elementos através de um caso de estudo. O roteiro visa informar o cliente sobre o processo de auditoria, enquanto o manual orienta o auditor na sua execução. Desta forma, estabelece-se um processo para a realização de auditorias adaptável a clientes de diferentes dimensões e recursos, incluindo grandes empresas e PMEs, mediante a seleção dos controlos relevantes para cada caso.

4.1.2 Pesquisa Levantamento Estado da Arte

Após a definição dos objetivos, procedeu-se à fase de investigação e levantamento do estado da arte. A pesquisa bibliográfica foi realizada utilizando motores de busca académicos, com destaque para o Google Scholar, e ferramentas de análise de literatura como Litmaps e Connected Papers para identificar trabalhos relevantes. As principais palavras-chave utilizadas na pesquisa incluíram "*cybersecurity*", "*security audits*", "PME"(ou "SME"), bem como os nomes de *frameworks* e normas como "NIST", "ISO", "QNRCS", "CIS", e termos relacionados.

Além de artigos científicos que forneceram a base teórica e exemplos práticos, foram consultadas normas internacionais (série ISO/IEC 27000, ISO 19011), guias e *frameworks* de referência (CIS, NIST), referenciais nacionais (QNRCS) e europeus (ENISA, RGPD). A escolha destas fontes específicas justifica-se pela necessidade de basear o trabalho nos *standards* e melhores práticas reconhecidas internacionalmente e adaptadas ao contexto nacional/europeu. Esta abordagem visou garantir que o roteiro e o manual desenvolvidos fossem não só academicamente fundamentados, mas também alinhados com as práticas de mercado e aplicáveis a diferentes contextos organizacionais, nomeadamente às PMEs, conforme os objetivos definidos. A análise cruzada destas fontes permitiu extrair os elementos essenciais para a construção das ferramentas de auditoria propostas.

4.2 Fase 2 - Desenvolvimento

A Fase 2 centra-se no desenvolvimento do roteiro de auditoria adaptado às necessidades específicas do cliente, definindo os controlos, a metodologia e os recursos necessários para garantir a eficácia do processo. Esta fase inclui também a criação de um manual para orientar o auditor e o desenvolvimento de uma plataforma de auditoria para facilitar o registo e o acompanhamento das ações realizadas.

4.2.1 Metodologia de Desenvolvimento do Roteiro de Auditoria

Para concretizar o desenvolvimento do roteiro de auditoria adota-se uma metodologia estruturada que garante a sua adaptação às especificidades do cliente e ao contexto das Pequenas e Médias Empresas (PME). Esta metodologia compreende três etapas interdependentes: investigação de *frameworks*, seleção e justificação dos controlos de segurança, e desenvolvimento das abordagens de avaliação. O objetivo final é criar um roteiro robusto, eficaz e adaptado que sirva de base para a auditoria, otimizando a segurança e a resiliência das organizações.

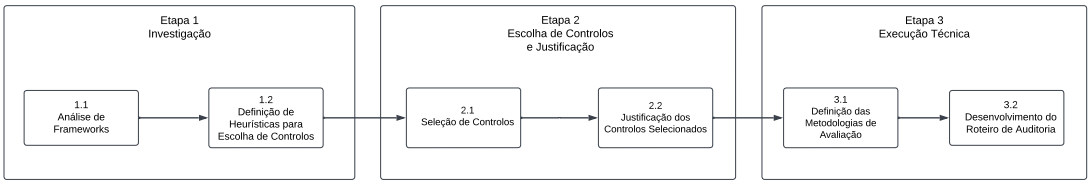

Figura 4.2: *Descrição da metodologia do roteiro de auditoria associado à Fase 2 - Desenvolvimento*

Etapa 1 - Investigação

O processo de criação do roteiro, conforme ilustrado pela Figura 4.2, tem início com a análise de várias metodologias de auditoria disponíveis na área. O objetivo desta análise é comparar as diferentes abordagens seguidas, de modo a extrair ideias e boas práticas que servirão de base para o desenvolvimento da metodologia de auditoria.

Uma parte importante das auditorias de segurança são os controlos que serão avaliados durante as auditorias. Antes da seleção dos controlos, são definidas as heurísticas que irão orientar esse processo. Estas heurísticas são utilizadas para selecionar os controlos mais relevantes para as PMEs.

Etapa 2 - Seleção e Justificação de Controlos

A Etapa 2 começa com a seleção dos controlos a utilizar na auditoria. Com base nas *frameworks* ou normas previamente analisadas, bem como nas heurísticas definidas na etapa anterior, são selecionados os controlos mais adequados ao contexto das PMEs. Este processo garante que os controlos selecionados são os mais eficazes, sem sobrecarregar as organizações.

Além disso, são descritas as razões para a escolha dos controlos, de modo a explicar como contribuem para a cibersegurança e a resiliência das PMEs.

Etapa 3 - Execução Técnica

Esta etapa é dedicada à definição detalhada das metodologias de avaliação. Foram estabelecidas três componentes centrais: primeiro, uma abordagem para determinar a criticidade de cada controlo de segurança e calcular a exposição global ao risco com base no seu nível de implementação; segundo, um método para classificar o risco revelado por cada atividade técnica da auditoria, com base nas evidências específicas encontradas; e terceiro, um sistema para agregar estas diferentes avaliações numa pontuação e classificação final que representa a postura de segurança global da empresa. A formalização prévia destas metodologias assegura a consistência, objetividade e clareza na avaliação e na comunicação dos resultados subsequentes.

Seguidamente, avança-se para o desenvolvimento do roteiro de auditoria propriamente dito. Este roteiro será baseado nas *frameworks* e normas previamente estudadas, mas será adaptado às necessidades específicas do cliente e ao contexto das PMEs para

garantir que os controlos selecionados são os mais relevantes e eficazes para cada cenário.

4.2.2 Definição do Manual do Auditor

O objetivo deste manual é fornecer ao auditor um guia claro e completo para a realização de todas as fases da auditoria. O manual descreve todas as etapas do processo, incluindo as ferramentas e recursos a utilizar em cada etapa. Além disso, são especificados os resultados de cada fase para garantir que o auditor tenha uma compreensão clara das expectativas e das tarefas a realizar. Este manual servirá de apoio prático, permitindo ao auditor seguir as etapas de forma estruturada e consistente, com o objetivo de garantir a qualidade e a eficácia do processo de auditoria.

4.2.3 Desenvolvimento da Aplicação Web de Suporte às Auditorias

Durante a auditoria, os auditores vão utilizar a plataforma online, desenvolvida especificamente para este contexto, que permite registar o que foi feito, como foi realizado e os resultados obtidos em cada etapa do processo. Desta forma, todas as informações serão organizadas de forma clara, e tanto o auditor como o cliente vão ter acesso a um resumo pormenorizado e bem estruturado de todo o processo da auditoria.

4.3 Fase 3 - Validação

A Fase 3 - Validação (Figura 4.1) centra-se na validação da metodologia de auditoria desenvolvida, incluindo o roteiro, os documentos e os processos associados, para garantir o seu alinhamento com os objetivos estabelecidos. Através de testes rigorosos e da implementação de melhorias contínuas, esta fase tem como objetivo assegurar que a metodologia é eficaz, prática e aplicável a diferentes contextos, identificando eventuais lacunas e ajustando os procedimentos conforme necessário. A aplicação prática e a demonstração desta fase são detalhadas no Capítulo 6.

4.3.1 Testes e Validação

Após a conclusão da primeira versão dos documentos de auditoria, será iniciada a fase de testes e validação. O objetivo desta fase é testar a metodologia de auditoria num ambiente controlado para validar a eficácia do processo, identificar eventuais lacunas ou pontos fracos e garantir que todas as etapas estão alinhadas com os objetivos definidos. Os resultados desta fase permitirão introduzir melhorias, ajustar procedimentos e otimizar a metodologia para garantir a sua adequação a diferentes contextos e necessidades.

4.3.2 Implementação de melhorias

Os documentos e o processo de auditoria serão continuamente atualizados e melhorados com base nos resultados dos testes. Serão introduzidas melhorias com base no *feedback* recolhido na fase de testes, a fim de garantir que a metodologia responde às necessidades práticas e que todas as fases do processo são otimizadas para maximizar a sua eficácia e aplicabilidade.

5
Desenvolvimento

O presente capítulo dedica-se ao detalhe do desenvolvimento da Fase 2 do projeto, focando-se na criação de uma metodologia de auditoria de segurança da informação otimizada para as necessidades específicas das Pequenas e Médias Empresas (PME). Para tal, este capítulo estrutura-se em três pilares fundamentais: a Metodologia de Desenvolvimento do Roteiro de Auditoria (que abrange a investigação, seleção de controlos e definição de métodos de avaliação), a Criação do Manual do Auditor (essencial para padronizar e guiar o processo), e o Desenvolvimento da Aplicação Web de suporte às auditorias (uma plataforma concebida para otimizar a execução e gestão das auditorias).

5.1 Metodologia de Desenvolvimento do Roteiro de Auditoria

A metodologia de desenvolvimento do roteiro de auditoria, presente na Figura 5.1, centra-se na pesquisa, seleção e justificação dos controlos de segurança mais adequados às necessidades específicas das PME. Através da análise de *frameworks* reconhecidas como a ISO/IEC 27001 [12], o NIST SP 800-115 [8] e o CIS Controls [19], foi desenvolvido um roteiro estruturado que permite identificar e mitigar eficazmente os riscos, adaptado às capacidades e limitações destas organizações. Esta fase envolve a seleção cuidadosa dos controlos, a justificação das escolhas feitas e a construção de um roteiro de auditoria que promova uma abordagem clara e eficaz da segurança da informação.

5.1.1 Etapa 1 - Investigação

A Etapa 1, associada à Fase 2, tem como objetivo analisar e definir os elementos essenciais para o desenvolvimento do roteiro de auditoria. Nesta fase, são exploradas as *frameworks* relevantes para criar o roteiro de auditoria e para selecionar os controlos adequados para a segurança da informação nas PME. Esta fase está dividida em duas partes: Análise das *Frameworks* e a Definição de Heurísticas para a Escolha de Controlos. Ambas as partes serão detalhadas a seguir.

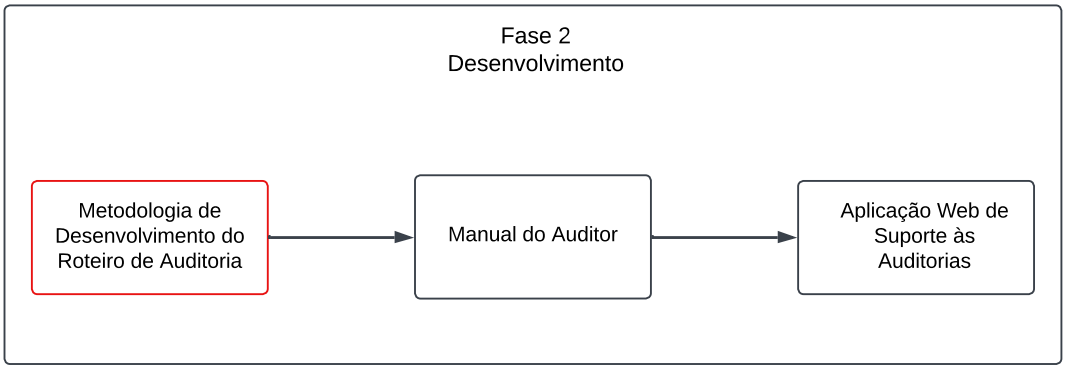

Figura 5.1: *Definição do Roteiro de Auditoria para o Cliente - Fase 2*

Etapa 1.1 - Análise de *Frameworks*

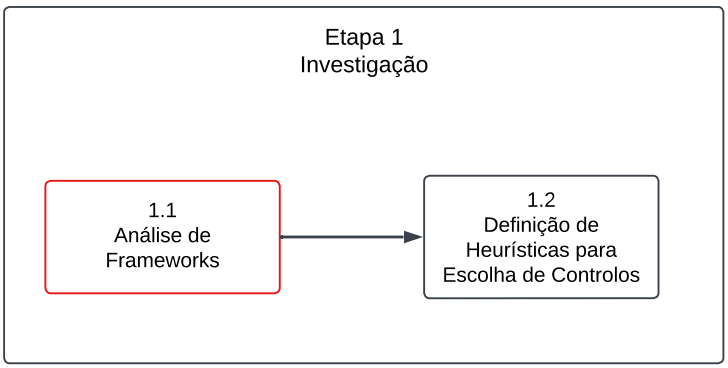

Figura 5.2: *Análise de Frameworks - Etapa 1.1*

Tendo por base as *frameworks* relevantes para a cibersegurança e auditorias de segurança apresentadas na Capítulo 2, esta secção foca-se na sua análise detalhada (Figura 5.2). A partir desta análise serão extraídas ideias, melhores práticas e diretrizes que irão guiar o desenvolvimento do roteiro de auditoria.

***Frameworks* para Cibersegurança:**

- A norma ISO/IEC 27001:2013 [17] foi utilizada como referência para identificar os controlos do seu Anexo A que melhor correspondiam aos critérios definidos para a auditoria. Estes controlos serviram de ponto de partida para selecionar os aspetos essenciais da segurança da informação a avaliar. Os controlos identificados serão depois mapeados para os controlos do Quadro Nacional de Referência para a Cibersegurança (QNRCS) [24], assegurando uma integração coerente entre as orientações internacionais e a realidade nacional.
- A implementação do controlo 3, "Proteção de Dados", do *CIS Controls* [19], foi fundamental para garantir a segurança no tratamento dos dados durante a auditoria. Este controlo apresenta uma abordagem estruturada para a identificação,

classificação e tratamento seguro dos dados, incluindo a aplicação de cifragem e a gestão do ciclo de vida dos dados, desde a sua recolha até à sua eliminação.

- O QNRCS [24] foi utilizado como base para selecionar os controlos mais adequados ao contexto nacional, garantindo a conformidade com as práticas de segurança recomendadas. Uma das suas principais vantagens é o facto de cada controlo estar mapeado para múltiplas referências internacionais, como o CIS Controls, COBIT 5 [54], ISO/IEC 27001:2013 [17] e NIST SP 800-53 Rev. 4 [9]. Esse mapeamento permite que a seleção dos controlos, não apenas cumpra com as diretrizes nacionais, mas também alinhe indiretamente a auditoria com diversas *frameworks* reconhecidas globalmente. Ao utilizar os controlos do QNRCS, o roteiro beneficia de uma base sólida, que incorpora as melhores práticas de diversas metodologias, garantindo uma abordagem coerente e em conformidade com as normas e recomendações mais utilizadas no setor.

***Frameworks* para Auditorias:**

- A NIST SP 800-115 [8] foi utilizado como referência principal para o desenvolvimento do roteiro de auditoria proposto, devido à sua abordagem abrangente e detalhada na realização de avaliações de segurança. Este documento fornece orientações específicas para as várias fases da auditoria, incluindo o planeamento, a descoberta da rede, a realização de testes técnicos e a análise dos resultados obtidos. A sua estrutura bem definida torna-o uma referência indispensável para auditorias de segurança, permitindo uma implementação organizada e facilmente ajustável a diferentes contextos.
  Além disso, a abordagem NIST SP 800-115 fornece uma visão prática da auditoria de segurança, descrevendo técnicas básicas como a análise de documentos, a revisão de registos, o *sniffing* de redes, o *scan* de vulnerabilidades e os testes de penetração. Estas orientações foram incorporadas no roteiro de auditoria desenvolvido para garantir que os processos definidos são suficientemente pormenorizados para permitir uma avaliação eficaz da segurança da informação.
  Embora a NIST SP 800-115 forneça diretrizes detalhadas para a realização de avaliações de segurança, a estrutura apresentada no documento não corresponde diretamente à de uma auditoria. Em vez de seguir esta organização, que abrange desde a descrição das técnicas individuais, até à comunicação dos resultados, foram extraídos os princípios e metodologias mais relevantes para construir o roteiro de auditoria proposto. Desta forma, a adaptação permitiu integrar as recomendações da NIST SP 800-115 de uma forma mais alinhada com os objetivos e a abordagem definidos.
  Além disso, o facto de a NIST SP 800-115 ser um documento de acesso público, permite que as suas recomendações sejam mais amplamente adotadas, fornecendo orientações técnicas essenciais para a realização de auditorias de segurança.
- O modelo CSAM [32] foi fundamental para a definição da pontuação de matu-

ridade, uma vez que forneceu uma *framework* robusta para avaliar a capacidade da organização em relação às práticas de cibersegurança. Utilizando os conceitos do CSAM, foi possível adaptar e aplicar uma avaliação final que considerou tanto os aspetos técnicos como organizacionais da empresa auditada, garantindo uma análise holística e objetiva do seu nível de maturidade em segurança da informação.

- O CIS *Risk Assessment Method* [33] foi utilizado para criar a matriz de risco, com ênfase na identificação, classificação e priorização dos riscos, garantindo assim uma avaliação clara e precisa do estado de segurança das PME.

Etapa 1.2 - Definição de Heurísticas para Escolha de Controlos

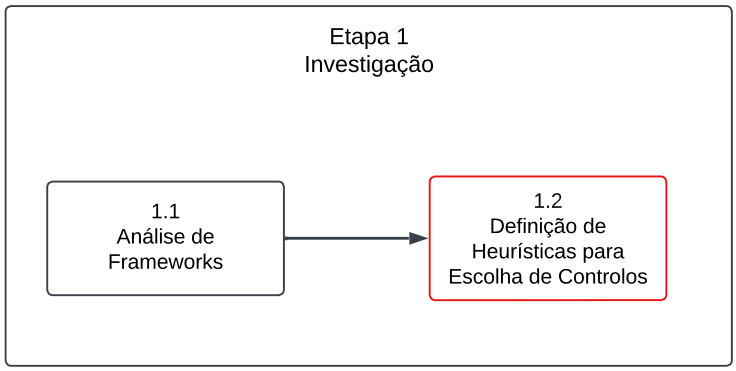

Figura 5.3: *Definição de Heurísticas para Escolha de Controlos - Etapa 1.2*

Para selecionar os controlos a serem analisados na auditoria, foram estabelecidos uma série de critérios, com base nas recomendações do trabalho [55], com o objetivo de garantir que a escolha seja adequada às necessidades das PME (Figura 5.3). Estes princípios levam em conta aspetos como a viabilidade de implementação em pequenas empresas, a relevância frente aos ciberataques mais comuns e a simplicidade de adaptação aos recursos já disponíveis nas organizações, sem a necessidade de adquirir infraestruturas adicionais ou de estabelecer uma estrutura formal interna. Estes critérios incluem:

- Não será necessário adquirir componentes de infraestruturas, como edifícios ou equipamentos específicos de redes;
- As PME não precisam de ter uma estrutura formal de recursos humanos e/ou empresariais já implementada;
- Os controlos selecionados devem focar-se na avaliação e mitigação dos ciberataques mais comuns identificados;
- Não será obrigatório implementar procedimentos de recuperação de desastres ou continuidade de negócio, dado que estas áreas não são prioritárias para pequenas empresas ou para organizações;

- Considerando que a maioria das PME não possuem um modelo sólido de processos empresariais, os controlos incluídos na metodologia proposta evitaram impor uma organização formal obrigatória dentro destas empresas.

De acordo com [55], os ciberataques mais comuns mencionados são:

- Ataques de engenharia social, como *phishing*, *malware*, *malware* móvel e *ransomware*;
- Ameaças relacionadas com políticas de gestão, nomeadamente palavras-passe fracas, mecanismos de autenticação fracos e controlos de acesso inadequados;
- Ameaças internas promovidas por funcionários, ex-funcionários, contratantes ou parceiros de negócios;
- Ameaças associadas ao *hardware*, como dispositivos pessoais dos colaboradores ou equipamentos críticos que suportam os sistemas de informação e serviços conexos (por exemplo, servidores web e de bases de dados);
- Ameaças relacionadas com *software*, causadas por aplicações de terceiros instaladas nos sistemas;
- *Distributed Denial-of-Service* (DDoS), com impacto significativo nas PMEs com uma presença online mais robusta;
- Exploração de informações confidenciais por parte de funcionários para roubar ou perturbar a atividade da empresa;
- Exposição involuntária a ciberataques devido ao não cumprimento de procedimentos de segurança por parte dos trabalhadores.

Esta lista será utilizada como referência para definir as heurísticas que orientarão a seleção dos controlos a auditar. Assim, garante-se que a auditoria seja abrangente, mas ao mesmo tempo realista e adaptada às principais necessidades das PMEs.

Com base nas heurísticas definidas, o presente trabalho adota a seleção de controlos do Anexo A da norma ISO/IEC 27001:2013, proposta por [55], por ser a que melhor se alinha com os critérios estabelecidos:

- (A.5) Políticas de segurança da informação;
- (A.8) Gestão de ativos;
- (A.9) Controlo de acessos;
- (A.10) Criptografia;
- (A.12) Segurança das operações;
- (A.13) Segurança nas comunicações;
- (A.14) Aquisição, desenvolvimento e manutenção de sistemas;
- (A.18) Conformidade.

A norma ISO/IEC 27001:2013 foi utilizada em detrimento da versão mais recente pelo facto de a versão atual do QNRCS ainda estar alinhada com a norma de 2013. Sendo o QNRCS a base para a seleção e mapeamento dos controlos neste trabalho, optou-se por manter a coerência com os controlos definidos nesta versão. Esta abordagem visa evitar incoerências que poderiam surgir da adoção de uma versão mais

recente da norma que não seja ainda compatível com o QNRCS utilizado neste contexto.

5.1.2 Etapa 2 - Escolha de Controlos e Justificação

A Etapa 2 (Figura 5.4) tem como objetivo a seleção e justificação dos controlos a serem implementados, considerando as necessidades específicas das PME e a sua capacidade de aplicar medidas de segurança adequadas. Esta fase é dividida em duas partes: a escolha dos controlos mais relevantes e a justificação das decisões tomadas, abordando tanto os controlos selecionados como os que foram excluídos com base nas características e limitações das PME.

Etapa 2.1 - Seleção de Controlos

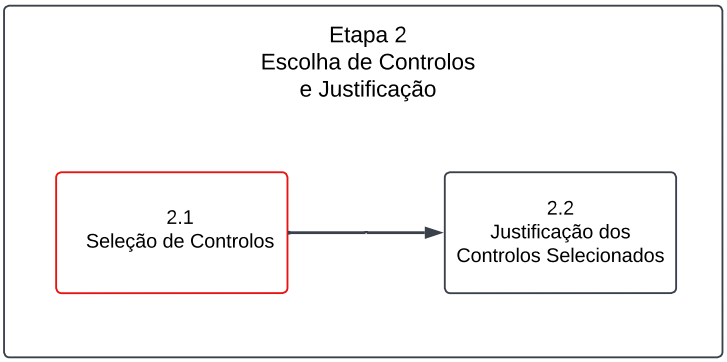

Figura 5.4: *Seleção de Controlos - Etapa 2.1*

A Figura 5.5 apresenta o diagrama do processo de seleção e correlação dos controlos, onde foi realizada a seleção dos controlos da ISO e a correspondência com os controlos do QNRCS. O processo incluiu a consolidação dos controlos, a avaliação de controlos adicionais e a correlação entre as versões da ISO/IEC 27002:2013 e 2022, com o objetivo de integrar os controlos do QNRCS de forma eficaz.

O Apêndice A expande a análise para além do referencial ISO/IEC 27001:2013, apresentando tabelas de mapeamento. Estas incluem o "Mapeamento dos controlos do QNRCS 2020 em relação aos controlos das normas ISO"e as "Correlações entre controlos da ISO/IEC 27002:2013, ISO/IEC 27002:2022 e QNRCS 2020 selecionados". Desta forma, o apêndice fornece uma perspetiva detalhada das interligações entre os controlos do QNRCS selecionados, os controlos da norma ISO/IEC 27002:2022, e as suas correspondências com as versões de 2013 e 2022 da norma ISO/IEC 27002.

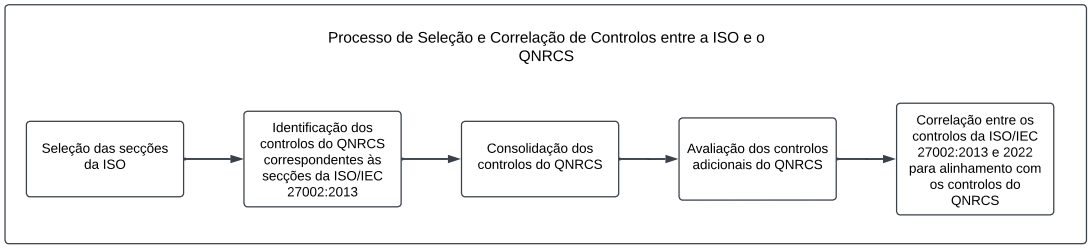

Figura 5.5: *Processo de Seleção e Correlação de Controlos entre a ISO e o QNRCS*

A Figura 5.6 apresenta os controlos do QNRCS que foram selecionados, com base nas secções A.5, A.8, A.9, A.10, A.12, A.13, A.14 e A.18 do Anexo A da ISO/IEC 27001:2013. No total, foram identificados 53 controlos relevantes para a auditoria, descritos em detalhe no Apêndice B. É importante notar que, em alguns casos, os controlos do QNRCS agregam múltiplos controlos da ISO/IEC 27001:2013, consolidando múltiplos aspetos de segurança num único controlo dentro do QNRCS.

Identificar	Proteger	Detetar	Responder
ID.GA-1	PR.GA-1	DE.AE-1	RS.AN-1
ID.GA-2	PR.GA-2	DE.AE-2	RS.MI-1
ID.GA-3	PR.GA-3	DE.AE-3	RS.MI-2
ID.GA-5	PR.GA-4	DE.AE-4	RS.MI-3
ID.AO-4	PR.GA-5	DE.MC-1	
ID.GV-1	PR.GA-6	DE.MC-3	
ID.GV-2	PR.GA-7	DE.MC-4	
ID.AR-1	PR.FC-1	DE.MC-7	
ID.AR-4	PR.FC-2	DE.MC-8	
ID.GR-1	PR.SD-1	DE.PD-2	
ID.GR-2	PR.SD-2	DE.PD-3	
ID.GR-3	PR.SD-3		
	PR.SD-4		
	PR.SD-5		
	PR.SD-7		
	PR.PI-1		
	PR.PI-2		
	PR.PI-3		
	PR.PI-4		
	PR.PI-5		
	PR.PI-6		
	PR.PI-12		
	PR.TP-2		
	PR.TP-3		
	PR.TP-4		
	PR.TP-5		

Figura 5.6: *Controlos Selecionados*

Etapa 2.2 - Justificação dos Controlos Selecionados

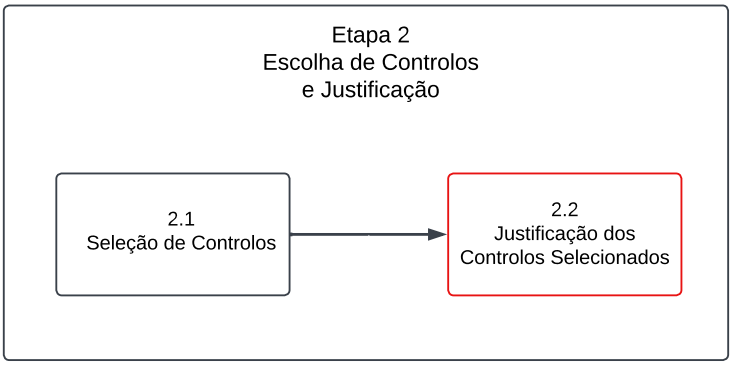

Figura 5.7: *Justificação dos Controlos Selecionados - 2.2*

Nesta etapa (Figura 5.7), são apresentadas as razões para a seleção das secções consideradas mais adequadas no contexto de uma PME, tendo em conta as suas necessidades e limitações específicas:

A.5 - Políticas de segurança da informação: A definição de políticas claras e acessíveis permite que as PMEs estabeleçam uma base de segurança que seja prática e aplicável, sem a necessidade de uma estrutura formal complexa. Isso ajuda a mitigar ciberataques comuns, como *phishing* e *malware*, sem sobrecarregar a organização com procedimentos excessivamente formais.

A.8 - Gestão de ativos: A gestão eficaz de ativos, mesmo em PMEs com recursos limitados, permite identificar e proteger os ativos críticos da organização, o que é essencial para prevenir perdas de dados e garantir a proteção de informações sensíveis, atendendo à necessidade de mitigar riscos comuns com baixo custo.

A.9 - Controlo de acessos: O controlo de acessos é crucial para proteger os dados e sistemas das PMEs contra acessos não autorizados. Esta cláusula garante que os direitos de acesso são atribuídos de forma adequada, minimizando o risco de intrusão ou fuga de dados, um ataque frequentemente utilizado pelos cibercriminosos.

A.10 - Criptografia: A criptografia assegura que os dados sensíveis permaneçam protegidos durante a transmissão e no momento em que são armazenados. Para PMEs, que não possuem grandes infraestruturas de segurança, a utilização da criptografia é uma solução acessível e eficaz para proteger dados críticos e evitar a sua exposição durante um ciberataque.

A.12 - Segurança das operações: Esta cláusula assegura a implementação de medidas de segurança nas operações diárias da empresa, o que é essencial para prevenir ataques que podem explorar falhas operacionais, como *malware* que procura explorar sistemas desatualizados ou configurações inadequadas, um problema comum em empresas de menores dimensões.

A.13 - Segurança nas comunicações: A proteção das comunicações entre sistemas e indivíduos é importante para impedir ataques, como interceção de dados e ataques *Man-in-the-middle* (MITM) [56]. As PME que não têm uma estrutura de rede robusta precisam de garantir que as comunicações dentro e fora da empresa são seguras, minimizando o risco dos dados sensíveis serem comprometidos.

A.14 - Aquisição, desenvolvimento e manutenção de sistemas: Esta cláusula garante que os sistemas adquiridos ou desenvolvidos pelas PME cumprem os critérios mínimos de segurança, o que é particularmente importante para as empresas que não dispõem de uma equipa técnica de segurança dedicada. Isto ajuda a evitar violações de segurança devido à utilização de software vulnerável ou desatualizado.

A.18 - Conformidade: Embora não seja obrigatório ter uma estrutura formal de conformidade, garantir o cumprimento das leis e regulamentações relevantes é fundamental para mitigar riscos legais e de cibersegurança, especialmente para as PMEs que, mesmo sem processos formais de recuperação de desastres ou continuidade de negócios, devem assegurar a proteção dos seus dados de acordo com as exigências legais de privacidade e segurança.

De seguida, justifica-se a exclusão das restantes secções, uma vez que não foram consideradas as mais adequadas ao contexto das PME:

A.6 - Organização da segurança da informação: A gestão da segurança da informação nas PME não exige uma estrutura organizacional complexa, como previsto nesta cláusula. A implementação de controlos simples, como as políticas de segurança e a gestão de ativos, já oferecem os elementos essenciais para enfrentar os riscos de segurança sem a necessidade de esforços organizacionais adicionais que podem ser dispendiosos para as empresas mais pequenas.

A.7 - Segurança dos recursos humanos: Embora a segurança dos recursos humanos seja importante, as PME podem não ter recursos suficientes para implementar políticas e formação pormenorizadas para todos os funcionários. A prioridade da segurança será focada em áreas mais diretamente relacionadas à proteção de dados e sistemas, como o controlo de acesso e a cifragem.

A.11 - Segurança física e ambiental: A segurança física é um aspeto fundamental em organizações de maior dimensão, mas para as PMEs, que frequentemente operam em espaços mais pequenos e com infraestrutura limitada, o foco recai mais sobre a proteção digital. Além disso, as PMEs já implementam controlos básicos de segurança física, como o bloqueio de salas e dispositivos.

A.15 - Relações com fornecedores: Embora a segurança nas relações com os fornecedores seja importante, muitas PME não têm uma rede extensa de fornecedores ou parcerias complexas que exijam uma análise de segurança pormenorizada.

A.16 - Gestão de incidentes de segurança da informação: Embora a gestão de incidentes seja fundamental, as PME podem não ter os recursos necessários para criar

planos formais de resposta a incidentes ou equipas específicas. A auditoria centrou-se em controlos mais acessíveis e práticos para atenuar os riscos.

A.17 - Aspetos de segurança da informação na gestão da continuidade dos negócios: Para as PME, que muitas vezes operam sem planos formais de continuidade das atividades, a implementação de controlos de continuidade das atividades pode ser vista como um custo adicional. As medidas de segurança escolhidas abordam diretamente os ciberataques mais comuns, como os ataques de *ransomware*, sem a necessidade de um plano de continuidade formal.

Adicionalmente aos controlos que se agrupam nos domínios específicos do Anexo A (como A.5, A.8, A.9, A.10, A.12, A.13, A.14 e A.18), foram incluídos controlos considerados fundamentais para uma base de segurança robusta.

Primeiramente, foram incluídos os controlos ID.GR-1, ID.GR-2 e ID.GR-3. Estes controlos são de natureza estratégica e não correspondem a medidas de segurança específicas, mas sim ao estabelecimento do próprio processo de gestão de risco.

É importante distinguir as duas partes principais da norma ISO/IEC 27001:

- As Cláusulas principais (4 a 10) definem os requisitos obrigatórios para criar e gerir o Sistema de Gestão de Segurança da Informação (o "como fazer a gestão");
- O Anexo A fornece um catálogo de controlos de segurança que podem ser selecionados para mitigar riscos (o "o que implementar").

Dado que os controlos ID.GR definem o processo de gestão de risco, o QNRCS alinha-os corretamente com as cláusulas principais da norma (como a 6.1.3 – Tratamento de riscos de segurança da informação, 8.3 – Tratamento de riscos de segurança da informação e 9.3 – Análise crítica pela direção), que são precisamente as que exigem a existência e gestão de um processo robusto de tratamento de risco.

Para além destes, foram incluídos outros 6 controlos de secções não priorizadas, por serem considerados essenciais. Embora a seleção principal privilegie a simplicidade para as PME, a inclusão destes controlos justifica-se pela necessidade de estabelecer uma base mínima de resiliência. No atual panorama de cibersegurança, certas medidas são fundamentais para mitigar riscos críticos, mesmo que se desviem da abordagem inicial focada em evitar complexidade.

Os 6 controlos adicionais e as suas respetivas justificações correspondem aos seguintes:

- PR.GA-2: Devem existir controlos de acesso físico às redes e sistemas de informação (A11).
  - Foi incluído para garantir que a segurança física das infra-estruturas digitais não é negligenciada. As PME não estão imunes a riscos físicos, como o roubo de equipamento ou o acesso não autorizado a sistemas. A implementação de controlos simples e eficazes nesta área pode evitar danos muito maiores, como a perda de dados sensíveis.

- PR.FC-2: Os utilizadores com acesso privilegiado devem compreender quais são os seus papéis e responsabilidades (A6 e A7).
  - Foi acrescentado porque, mesmo em organizações mais pequenas, as permissões privilegiadas representam um risco significativo se não forem devidamente controladas. Uma definição clara dos papéis pode evitar o uso indevido ou erro humano, que pode ser fatal no contexto de um ciberataque, ajudando a minimizar o risco sem necessidade de uma estrutura organizacional complexa.
- PR.PI-5: As políticas e regulamentações associadas à operacionalização dos ambientes físicos dos ativos da organização devem ser seguidas (A11).
  - Foi incluído como uma medida preventiva. Embora as PME não necessitem de regulamentos formais, o funcionamento destes ambientes físicos sem um mínimo de normalização pode criar enormes vulnerabilidades. A garantia de que determinadas práticas são seguidas pode evitar que falhas operacionais conduzam a incidentes de segurança.
- PR.TP-5: Devem ser implementados mecanismos para cumprir os requisitos de resiliência em situações adversas (A17).
  - Foi incluído com o objetivo de preparar as PME para situações adversas. A implementação da resiliência não requer infra-estruturas pesadas ou processos formais complexos, mas sim a preparação para cenários críticos, o que é cada vez mais importante num mundo onde as ciberameaças são constantes.
- DE.AE-4: O impacto dos eventos deve ser classificado (A16).
  - Foi incluído para que as PME possam ter uma ideia clara de como as diferentes ameaças podem afetar os seus negócios. Mesmo sem uma estrutura formal, esta avaliação pode ser efetuada de forma simples, dando prioridade aos riscos mais imediatos e ajustando as defesas em conformidade.
- DE.MC-1: As redes e sistemas de informação devem ser monitorizados para detetar potenciais incidentes (sem correspondência direta).
  - Foi adicionado por ser essencial para as PME detetarem atempadamente atividades anómalas ou maliciosas. Ter uma visibilidade mínima sobre sistemas e redes, mesmo que básica, é crucial para permitir uma resposta rápida a incidentes e limitar danos significativos.

Deste modo, embora não estejam diretamente em conformidade com os pressupostos iniciais, a inclusão destes controlos destina-se a garantir que as PMEs consigam atingir um nível mínimo de cibersegurança e resiliência sem a necessidade de processos excessivamente burocráticos, satisfazendo as necessidades atuais de proteção de dados e continuidade das atividades.

5.1.3 Etapa 3 - Execução Técnica

Esta fase (Figura 5.8) do processo abrange a definição das metodologias de avaliação das várias fases da auditoria e o desenvolvimento do Roteiro de Auditoria.

Etapa 3.1 - Definição das Metodologias de Avaliação

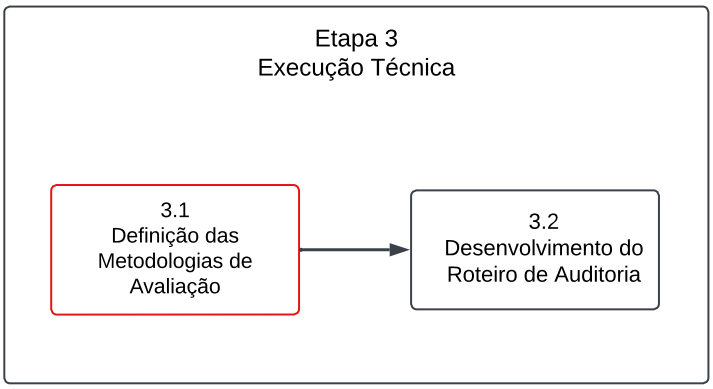

Figura 5.8: *Definição das Metodologias de Avaliação - Etapa 3.1*

Avaliação da Criticidade e Exposição ao Risco

Primeiro, define-se a classificação de importância (ou criticidade) atribuída a cada controlo de segurança. Esta classificação, que varia em níveis de 1 a 5 (onde 1 representa o nível mais baixo de criticidade e 5 o nível mais crítico), é apresentada nas Figura 5.9a e Figura 5.9b, e baseia-se numa interpretação da criticidade e impacto potencial de cada controlo. Dado que o QNRCS não define esta escala numérica, a classificação serve como um guia geral sobre a relevância de cada controlo (c) para a segurança, risco e continuidade de uma organização. Este valor será referido como $Crit(c)$.

O significado de cada nível de importância ($Crit(c)$) é o seguinte:

- Nível 5 (Crítica): Controlos fundamentais. A sua falha ou ausência tem impacto grave na segurança, operações ou conformidade. Implementação essencial e de prioridade máxima.
- Nível 4 (Elevada): Controlos cruciais para uma segurança robusta e mitigação significativa de riscos. A sua ausência representa uma lacuna considerável. Implementação fortemente recomendada.
- Nível 3 (Média): Controlos que representam boas práticas padrão. Contribuem para reduzir riscos moderados e melhorar a eficiência da segurança. Importantes para uma segurança madura.
- Nível 2 (Baixa): Controlos úteis que contribuem positivamente, mas são menos fundamentais. O impacto da sua falha é mais limitado ou específico.

- Nível 1 (Mínima): Controlos opcionais ou de baixo impacto geral. A sua ausência tem impacto negligenciável na maioria das organizações. Relevantes apenas em circunstâncias muito específicas.

Categoria	Controlo	Importância
Identificar (ID)	ID.GA-1	5 (Crítica)
	ID.GA-2	5 (Crítica)
	ID.GA-3	4 (Elevada)
	ID.GA-5	5 (Crítica)
	ID.AO-4	5 (Crítica)
	ID.GV-1	5 (Crítica)
	ID.GV-2	4 (Elevada)
	ID.AR-1	5 (Crítica)
	ID.AR-4	5 (Crítica)
	ID.GR-1	5 (Crítica)
	ID.GR-2	4 (Elevada)
	ID.GR-3	4 (Elevada)
Proteger (PR)	PR.GA-1	5 (Crítica)
	PR.GA-2	4 (Elevada)
	PR.GA-3	4 (Elevada)
	PR.GA-4	5 (Crítica)
	PR.GA-5	4 (Elevada)
	PR.GA-6	5 (Crítica)
	PR.GA-7	5 (Crítica)
	PR.FC-1	5 (Crítica)
	PR.FC-2	4 (Elevada)
	PR.SD-1	5 (Crítica)
	PR.SD-2	5 (Crítica)
	PR.SD-3	3 (Média)
	PR.SD-4	4 (Elevada)
	PR.SD-5	4 (Elevada)
	PR.SD-7	4 (Elevada)
	PR.PI-1	5 (Crítica)
	PR.PI-2	4 (Elevada)
	PR.PI-3	4 (Elevada)
	PR.PI-4	5 (Crítica)
	PR.PI-5	3 (Média)
	PR.PI-6	4 (Elevada)
	PR.PI-12	5 (Crítica)
	PR.TP-2	3 (Média)
	PR.TP-3	4 (Elevada)
	PR.TP-4	4 (Elevada)
	PR.TP-5	4 (Elevada)

(**a**) *Classificação dos Controlos de Segurança - 1*

Categoria	Controlo	Importância
Detetar (DE)	DE.AE-1	3 (Média)
	DE.AE-2	4 (Elevada)
	DE.AE-3	4 (Elevada)
	DE.AE-4	3 (Média)
	DE.MC-1	5 (Crítica)
	DE.MC-3	3 (Média)
	DE.MC-4	5 (Crítica)
	DE.MC-7	4 (Elevada)
	DE.MC-8	4 (Elevada)
	DE.PD-2	3 (Média)
	DE.PD-3	3 (Média)
Responder (RS)	RS.AN-1	4 (Elevada)
	RS.MI-1	5 (Crítica)
	RS.MI-2	4 (Elevada)
	RS.MI-3	3 (Média)

(**b**) *Classificação dos Controlos de Segurança - 2*

Figura 5.9: *Classificação dos Controlos de Segurança: (a) Controlo de Identificação e Proteção; (b) Controlo de Deteção e Resposta.*

Esta classificação de criticidade ($Crit(c)$) é então utilizada, em conjunto com o nível de implementação de cada controlo, para calcular a exposição global ao risco da organização. A metodologia adaptada para este cálculo, detalhada de seguida, utiliza

uma escala de implementação de quatro níveis para cada controlo.

Primeiramente, avalia-se o nível de implementação de cada controlo de segurança (c) incluído na auditoria. O cliente indica este nível de acordo com a seguinte escala: Nada Implementado, Pouco Implementado, Parcialmente Implementado ou Totalmente Implementado. A cada um destes níveis de implementação corresponde um Peso de Risco Residual $(Peso_{Risco}(c))$ que representa a fração da criticidade $Crit(c)$ que ainda contribui para o risco global. Especificamente, atribui-se $Peso_{Risco}(c) = 1.00$ para 'Nada Implementado', $Peso_{Risco}(c) = 2/3$ para 'Pouco Implementado', $Peso_{Risco}(c) = 1/3$ para 'Parcialmente Implementado', e $Peso_{Risco}(c) = 0.00$ para 'Totalmente Implementado'.

De seguida, calcula-se a Pontuação Total de Exposição ao Risco. Esta pontuação é obtida somando a criticidade ponderada de todos os controlos (c) avaliados. A criticidade de cada controlo $(Crit(c))$ é multiplicada pelo seu respetivo Peso de Risco Residual $(Peso_{Risco}(c))$. Sendo C_{Total} o conjunto dos 53 controlos avaliados, a Pontuação Total de Exposição ao Risco é dada por:

$$\text{Pontuação Total Exposição Risco} = \sum_{c \in C_{Total}} (Crit(c) \times Peso_{Risco}(c)) \tag{5.1}$$

Para normalizar esta pontuação, define-se o Risco Máximo Total $(Risco_{Max})$ como a soma da criticidade de todos os controlos, assumindo que nenhum está implementado $(Peso_{Risco}(c) = 1.0$ para todos os $c \in C_{Total})$. Com base na soma das criticidades $Crit(c)$ para os 53 controlos, tem-se:

$$Risco_{Max} = \sum_{c \in C_{Total}} Crit(c) = 224 \tag{5.2}$$

A Pontuação Total de Exposição ao Risco (Equação 5.1) representa o risco presente de forma granular.

Posteriormente, calcula-se a Média de Risco por Controlo Não Totalmente Implementado (designada por Média). Para tal, identifica-se primeiro o conjunto de controlos que não estão totalmente implementados (C_{NFI}), ou seja, aqueles classificados como Nada Implementado, Pouco Implementado ou Parcialmente Implementado. A Pontuação Total de Exposição ao Risco, calculada através da Equação 5.1, representa a soma do risco contribuído por estes controlos. Assim, a Média é obtida dividindo esta pontuação pelo número de controlos não totalmente implementados $(|C_{NFI}|)$, caso existam $(|C_{NFI}| > 0)$:

$$\text{Média} = \begin{cases} \frac{\sum_{c \in C_{Total}} (Crit(c) \times Peso_{Risco}(c))}{|C_{NFI}|} & \text{se } |C_{NFI}| > 0 \\ 0 & \text{se } |C_{NFI}| = 0 \end{cases} \tag{5.3}$$

Esta média representa a pontuação de risco média contribuída por cada controlo que não está totalmente implementado (ou seja, classificado como Nada Implemen-

tado, Pouco Implementado ou Parcialmente Implementado). Para o cliente, isto traduz a 'severidade' média das deficiências encontradas nesses controlos.

Por fim, calcula-se calcula-se a Percentagem de Exposição ao Risco. Este valor é obtido dividindo a Pontuação Total de Exposição ao Risco (Equação 5.1) pelo Risco Máximo Total ($Risco_{Max}$), conforme definido na Equação 5.2, e multiplicando o resultado por 100:

$$\text{Percentagem de Exposição ao Risco (\%)} = \left(\frac{\text{Pontuação Total Exposição Risco}}{Risco_{Max}} \right) \times 100 \tag{5.4}$$

A aplicação prática da metodologia é ilustrada através do seguinte cenário simulado. Assume-se um universo total de 53 controlos com $Risco_{Max} = 224$ (Equação 5.2). Suponha que 48 controlos estão "Totalmente Implementados" ($Peso_{Risco} = 0.0$), contribuindo com 0 para a pontuação total. Os 5 controlos restantes (C_{NFI}), com $|C_{NFI}| = 5$, e as suas respetivas avaliações são:

- Controlo 1: $Crit(c_1) = 5$, Nível=Nada Implementado ($Peso_{Risco}(c_1) = 1.0$);
- Controlo 2: $Crit(c_2) = 4$, Nível=Pouco Implementado ($Peso_{Risco}(c_2) = 2/3$);
- Controlo 3: $Crit(c_3) = 3$, Nível=Parcialmente Implementado ($Peso_{Risco}(c_3) = 1/3$);
- Controlo 4: $Crit(c_4) = 2$, Nível=Pouco Implementado ($Peso_{Risco}(c_4) = 2/3$);
- Controlo 5: $Crit(c_5) = 1$, Nível=Parcialmente Implementado ($Peso_{Risco}(c_5) = 1/3$).

Aplicando a Equação 5.1, a Pontuação Total de Exposição ao Risco é:

$$\begin{aligned} \text{Pontuação Total} &= (5 \times 1.0) + (4 \times 2/3) + (3 \times 1/3) + (2 \times 2/3) + (1 \times 1/3) \\ &= 5.0 + \frac{8}{3} + 1 + \frac{4}{3} + \frac{1}{3} \\ &= \frac{31}{3} \approx 10.33 \end{aligned} \tag{5.5}$$

De seguida, utilizando a Equação 5.3, calcula-se a Média de Risco por Controlo Não Totalmente Implementado:

$$\text{Média} = \frac{31/3}{5} = \frac{31}{15} \approx 2.07 \tag{5.6}$$

Esta média indica que a contribuição média para o risco, por cada um destes 5 controlos não totalmente implementados, é de ≈ 2.07 pontos de criticidade ponderada. Por fim, aplicando a Equação 5.4 e usando o valor de $Risco_{Max} = 224$ (Equação 5.2), a Percentagem de Exposição ao Risco é:

$$\text{Percentagem (\%)} = \left(\frac{31/3}{224} \right) \times 100 = \left(\frac{31}{654} \right) \times 100 \approx 4.74\% \tag{5.7}$$

Com base neste cálculo da Percentagem de Exposição ao Risco (ex: 4.74%), a orga-

nização encontrar-se-ia no estado de segurança 'Segura', conforme a Tabela 5.1. Isto significa que 4.74% do risco potencial máximo, considerando a criticidade de todos os controlos, ainda está presente devido à implementação inexistente ou parcial dos mesmos. A Média de Risco por Controlo Não Totalmente Implementado, que neste exemplo é de 2.2, quantifica o impacto médio de cada falha de implementação. Um valor elevado neste indicador sinaliza uma maior gravidade média das lacunas, a qual pode derivar tanto da alta criticidade dos controlos afetados como de uma deficiência severa na sua implementação. Deste modo, o indicador, operando numa escala de 1 a 5, funciona como uma "criticidade efetiva"de cada controlo não conforme.

A Tabela 5.1 atribui ao Percentagem de Exposição ao Risco um **Nível de Risco** (numa escala de 1 a 5) correspondente a cada faixa de exposição. Este nível será posteriormente utilizado como a nota do Capítulo 3 para o cálculo da Avaliação Final da Empresa.

Tabela 5.1: *Escala de Referência para Exposição ao Risco*

Exposição ao Risco (%)	**Estado de Segurança**	**Interpretação**	**Nível de Risco**
0%	Muito Segura	Todos os controlos estão totalmente implementados. Risco residual mínimo.	1 (Informativo)
1% - 20%	Segura	Maioria dos controlos totalmente ou parcialmente implementados. Risco limitado.	2 (Baixo)
21% - 40%	Moderadamente Vulnerável	Vários controlos com implementação parcial, pouca ou nenhuma. Risco significativo.	3 (Moderado)
41% - 60%	Vulnerável	Muitos controlos com implementação parcial, pouca ou nenhuma. Risco alto.	4 (Elevado)
61% - 100%	Muito Vulnerável	Grande número de controlos não implementados ou pouco implementados. Risco crítico.	5 (Crítico)

Metodologia de Classificação de Risco por Atividade de Auditoria

Um dos pilares desta metodologia de avaliação é a classificação de risco atribuída a cada atividade técnica específica realizada durante a auditoria (por exemplo: Análise de Portos Abertos, Análise de Email, Teste de Penetração, etc.). Para garantir a objetividade, a consistência e a reprodutibilidade dos resultados, a classificação de risco para cada atividade não se baseia numa avaliação puramente subjetiva. Em vez disso, segue um processo estruturado e baseado em evidências, que obedece aos seguintes princípios gerais:

- **Definição de Critérios Específicos:** O primeiro passo consiste em definir, para

cada atividade técnica, critérios claros e específicos mapeados para diferentes níveis de risco (numa escala de 1 - Informativo a 5 - Crítico). Estes critérios baseiam-se nos tipos de evidências que podem ser obtidas durante a atividade (por exemplo: potencial de exploração de portos, tipo de dados comprometidos em emails, pontuação *Common Vulnerability Scoring System* (CVSS) de vulnerabilidades).

- **Atribuição de Pontuações e Níveis de Risco:** AA cada critério específico é associado um Nível de Risco qualitativo e uma Pontuação Atribuída ao Critério correspondente, que reflete a sua contribuição para o score final. A relação padrão utilizada é a seguinte:
  - Nível 1 - Risco Informativo: Pontuação Atribuída de 0.1;
  - Nível 2 - Risco Baixo: Pontuação Atribuída de 0.3;
  - Nível 3 - Risco Moderado: Pontuação Atribuída de 0.6;
  - Nível 4 - Risco Elevado: Pontuação Atribuída de 1.5;
  - Nível 5 - Risco Crítico: Pontuação Atribuída de 2.5.

  As tabelas de pontuação para cada tipo de atividade (ilustradas na Tabela 5.3, Tabela 5.5 e Tabela 5.7) definem formalmente estes critérios e as suas respetivas pontuações. Esta estrutura de pontuações foi definida de forma a que, se todos os critérios de risco (um para cada nível de 1 a 5) fossem identificados numa atividade, a aplicação da Equação 5.8 resultasse numa pontuação de 5.0 (sendo $0.1 + 0.3 + 0.6 + 1.5 + 2.5 = 5.0$), alinhando-se com o topo da escala qualitativa final.
- **Cálculo da Pontuação Numérica da Atividade:** A pontuação numérica de uma atividade é obtida através da soma direta das Pontuações Atribuídas aos Critérios para cada tipo de evidência detetada. Seja $E_{descoberta}$ o conjunto dos critérios de avaliação efetivamente aplicáveis a uma determinada atividade.
  É fundamental notar que cada critério de risco (ex: Baixo, Moderado, Elevado) contribui no máximo uma vez para a pontuação final, independentemente do número de evidências do mesmo tipo que sejam encontradas. Assim, por exemplo, a deteção de três vulnerabilidades 'Moderadas' resulta na adição da pontuação correspondente a 'Moderado' (0.6) uma única vez à soma.
  Esta regra é formalizada pela seguinte equação:

$$\text{Pontuação Numérica Atividade} = \sum_{e \in E_{descoberta}} (\text{PontuaçãoAtribuída}_e) \tag{5.8}$$

  As tabelas seguintes ilustram como os critérios, pesos e níveis de risco são definidos para diferentes tipos de atividades.

Tabela 5.3: *Tabela de Pontuação de Risco para Portos Abertos*

Critério de Avaliação	**Pontuação Atribuída**	**Nível de Risco (1 a 5)**
Identificação de portos abertos sem riscos conhecidos.	0.1	1 (Informativo)
Identificação de portos abertos que podem ser utilizadas em ataques comuns.	1.5	4 (Elevado)
Identificação de portos abertos com alto potencial de exploração em ataques.	2.5	5 (Crítico)

Tabela 5.5: *Tabela de Pontuação de Risco para Recolha de Informações online*

Critério de Avaliação	**Pontuação Atribuída**	**Nível de Risco (1 a 5)**
Referências públicas a funcionários (sem detalhes adicionais). Sem divulgação de emails.	0.1	1 (Informativo)
Redes sociais de colaboradores (sem informações sensíveis). Divulgação de emails públicos sem comprometimento.	0.3	2 (Baixo)
Estrutura organizacional, cargos e departamentos. Divulgação de emails comprometidos sem credenciais expostas.	0.6	3 (Moderado)
Divulgação de emails e números de telefone profissionais. Fugas de dados com credenciais associadas a contas de email.	1.5	4 (Elevado)
Divulgação de credenciais de acesso a sistemas críticos ou números de telefone pessoais de funcionários chave. Fugas de dados com credenciais recentes para contas de email altamente sensíveis.	2.5	5 (Crítico)

Tabela 5.7: *Tabela de Pontuação de Risco dos Testes de Penetração*

Critério de Avaliação	**Pontuação Atribuída**	**Nível de Risco**
Nenhuma falha significativa encontrada. Nenhum CVE relevante identificado.	0.1	1 (Informativo)
Vulnerabilidades de baixa relevância, sem impacto significativo. CVSS *score* menor ou igual a 3.9.	0.3	2 (Baixo)
Vulnerabilidades com impacto moderado, sem comprometer dados críticos. CVSS *score* entre 4.0 e 6.9.	0.6	3 (Moderado)
Acesso parcial a sistemas críticos ou dados sensíveis. CVSS *score* entre 7.0 e 8.9.	1.5	4 (Elevado)

Continua na página seguinte...

Tabela 5.8 (continuação): Tabela de Pontuação de Risco dos Testes de Penetração

Critério de Avaliação	**Pontuação Atribuída**	**Nível de Risco**
Controlo total dos sistemas ou acesso a dados altamente sensíveis. CVSS *score* maior ou igual 9.0.	2.5	5 (Crítico)

Como exemplo, considere-se o cálculo para a atividade de Testes de Penetração (Tabela 5.7). Suponha que, durante esta atividade, foram identificadas as seguintes evidências:

- Uma vulnerabilidade de baixa relevância (CVSS $\leq$ 3.9);
- Uma vulnerabilidade de impacto moderado (CVSS entre 4.0 e 6.9);
- Uma falha que permitiu acesso parcial a sistemas críticos (CVSS entre 7.0 e 8.9).

Mapeando cada evidência para o seu Nível de Risco e Pontuação Atribuída ao Critério correspondentes:

- Vulnerabilidade Baixa: $NivelRisco = 2$, Pontuação Atribuída = 0.3;
- Vulnerabilidade Moderada: $NivelRisco = 3$, Pontuação Atribuída = 0.6;
- Acesso Parcial (Elevado): $NivelRisco = 4$, Pontuação Atribuída = 1.5.

Calcula-se a Pontuação Numérica da Atividade usando a Equação 5.8:

$$\begin{aligned} \text{Pontuação Numérica (Teste Penetração)} &= 0.3 + 0.6 + 1.5 \\ &= 2.40 \end{aligned} \tag{5.9}$$

Portanto, a classificação de risco final reportada para esta atividade específica seria 2.4. Este valor será depois utilizado na avaliação geral da empresa.
Esta abordagem garante que a classificação de risco atribuída a cada atividade reflete diretamente as vulnerabilidades, exposições ou falhas concretas identificadas, reduzindo significativamente a ambiguidade e permitindo uma avaliação mais consistente da postura de segurança da organização em cada área técnica avaliada.

Sistema para a Avaliação Final da Empresa

Para consolidar os resultados das classificações de risco obtidas em cada atividade técnica da auditoria, foi definido um sistema para calcular a Avaliação Geral da Empresa. Esta métrica final agrega os diferentes resultados numa única pontuação que reflete a postura global de segurança da organização, conforme avaliado pela metodologia.

O cálculo baseia-se nas Classificações de Risco atribuídas a cada atividade de auditoria (detalhadas anteriormente). Estas atividades são agrupadas em três capítulos

principais do Manual do Auditor, cujo índice está disponível para consulta no Apêndice D.: Capítulo 3 ('Avaliação dos Controlos de Segurança'), Capítulo 4 ('Recolha de Informações e Identificação de Ativos') e Capítulo 5 ('Identificação e Avaliação de Riscos'). A importância relativa de cada um destes capítulos na avaliação global é refletida através de pesos específicos.

O Capítulo 5 do Manual do Auditor ('Identificação e Avaliação de Riscos'), que inclui atividades de exploração e testes mais aprofundados (como Teste de Penetração, SAST/DAST), recebe o maior peso, de 40%. Esta ponderação justifica-se pelo facto de estas ações tenderem a validar a explorabilidade de vulnerabilidades e a revelar os riscos com impacto mais direto e potencialmente severo na segurança da organização. Ao Capítulo 3 ('Avaliação dos Controlos de Segurança') atribui-se um peso substancial de 35%, reconhecendo que a robustez dos controlos fundamentais é crítica para uma postura de segurança resiliente e preventiva, formando a base essencial da proteção. Por fim, o Capítulo 4 ('Recolha de Informações e Identificação de Ativos'), abrangendo Reconhecimento, *Scanning* e Análise de Vulnerabilidades, recebe um peso de 25%. Este valoriza a importância da identificação da superfície de ataque e das potenciais fraquezas, mas considera que o risco real associado a estas descobertas é frequentemente confirmado pelas falhas nos controlos base (Capítulo 3) ou pela sua explorabilidade (Capítulo 5).

O processo de cálculo da Avaliação Geral, utilizando estes capítulos e os seus respetivos pesos, segue os seguintes passos:

Passo 1 - Cálculo das Pontuações por Capítulo do Manual do Auditor: Determina-se uma pontuação representativa para cada um dos capítulos principais:

- Pontuação da 'Avaliação dos Controlos de Segurança' (Capítulo 3): Dado que este capítulo contém apenas a atividade 3.1 (Avaliação de Controlos de Segurança), a pontuação deste capítulo (P_3) é diretamente a Classificação de Risco obtida para essa atividade específica, conforme a Equação 5.10.

$$P_3 = \text{Classificação Risco (Atividade 3.1)} \tag{5.10}$$

- Pontuação da 'Recolha de Informações e Identificação de Ativos' (Capítulo 4): Este capítulo agrega várias atividades (4.1.1 a 4.4). A sua pontuação (P_4) é calculada como a média das Classificações de Risco de todas as atividades pertencentes a este capítulo, como mostra a Equação 5.11. Seja N_4 o número de atividades no Capítulo 4 (11):

$$P_4 = \frac{\sum_{i \in \text{Atividades Cap. 4}} \text{Classificação Risco}_i}{N_4} \tag{5.11}$$

- Pontuação da 'Identificação e Avaliação de Riscos' (Capítulo 5): Similarmente, este capítulo agrupa as atividades 5.1.1 a 5.2.3. A sua pontuação (P_5) é a média das Classificações de Risco de todas as atividades que o compõem, calculada pela

Equação 5.12. Seja N_5 o número de atividades no Capítulo 5 (7):

$$P_5 = \frac{\sum_{j \in \text{Atividades Cap. 5}} \text{Classificação Risco}_j}{N_5} \tag{5.12}$$

Passo 2 - Cálculo da Avaliação Geral Ponderada: A Avaliação Geral da Empresa é calculada como uma média ponderada das pontuações dos três capítulos (P_3, P_4, P_5), obtidas respetivamente através das Equações 5.10, 5.11 e 5.12. Utilizam-se os pesos anteriormente justificados (35% para o Capítulo 3, 25% para o Capítulo 4 e 40% para o Capítulo 5). A fórmula para este cálculo é apresentada na Equação 5.13:

$$\text{Avaliação Geral} = (P_3 \times 0.35) + (P_4 \times 0.25) + (P_5 \times 0.40) \tag{5.13}$$

Passo 3 - Interpretação da Avaliação Geral: O resultado numérico da Avaliação Geral (tipicamente um valor entre 1 e 5) é então interpretado para fornecer uma classificação qualitativa final sobre o nível de segurança da empresa. Utiliza-se para isso a escala de referência apresentada na Tabela 5.9.

Tabela 5.9: *Interpretação da Avaliação Geral*

Avaliação Geral	Nível de Segurança	Interpretação
0.0 - 1.0	5 (Excelente)	Indica controlos globalmente eficazes e riscos residuais mínimos identificados nas atividades técnicas.
1.1 - 2.0	4 (Bom)	Indica uma base de controlos razoável e/ou riscos identificados de impacto limitado.
2.1 - 3.0	3 (Moderado)	Existem vulnerabilidades e/ou lacunas nos controlos que resultam em riscos significativos e requerem atenção.
3.1 - 4.0	2 (Preocupante)	Indica elevada exposição ao risco devido a falhas importantes nos controlos e/ou vulnerabilidades de alto impacto identificadas.
4.1 - 5.0	1 (Crítico)	Indica exposição muito elevada ao risco devido a falhas graves e generalizadas nos controlos e/ou vulnerabilidades críticas identificadas. Ação corretiva urgente é necessária.

Etapa 3.2 - Desenvolvimento do Roteiro de Auditoria

Durante esta fase (Figura 5.10) do processo, a estrutura do roteiro de auditoria de segurança foi desenvolvida com base no NIST SP 800-115 [8].

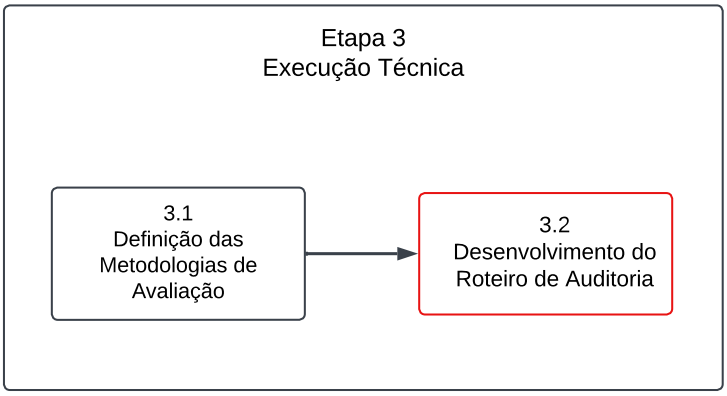

Figura 5.10: *Desenvolvimento do Roteiro de Auditoria - 3.2*

Objetivos do Roteiro de Auditoria de Segurança

Este roteiro de auditoria foi desenvolvido para transformar a complexidade da avaliação da segurança num processo fluido e orientado para os resultados. Em vez de uma abordagem rígida, optou-se por uma estrutura modular, que possibilita o seguimento lógico de cada fase e assegura que cada uma delas contribua de forma eficaz para a identificação e mitigação dos riscos. Esta organização modular também proporciona flexibilidade para se adaptar a diferentes realidades organizacionais, permitindo que o processo seja ajustado conforme as necessidades específicas de cada cliente. Para garantir clareza e eficiência, este roteiro segue uma estrutura bem definida, assegurando que os objetivos, responsabilidades e metodologias sejam claros desde o início. Dessa forma, todas as partes envolvidas têm uma visão transparente do processo, permitindo uma avaliação organizada e alinhada com as necessidades da organização.

Ao organizar o roteiro desta forma, pretende-se alcançar um equilíbrio entre o rigor técnico e a clareza, de modo a garantir que o cliente compreenda facilmente os passos da auditoria e a importância de cada fase no fortalecimento da segurança da informação.

Estrutura do Roteiro de Auditoria

De seguida, apresenta-se a estrutura do roteiro de auditoria:

- Planeamento e Preparação
  - Questionário pré-auditoria: Este questionário preliminar é essencial para a recolha de informações iniciais sobre o ambiente da organização e as expectativas da auditoria. O seu objetivo é fornecer à primeira reunião de planeamento dados relevantes, tornando-a mais focada e produtiva;
  - Desenvolvimento do Plano de Auditoria: Este plano abrangente serve como guia para toda a auditoria e define os objetivos, o âmbito detalhado (incluindo sistemas e exclusões) e a logística operacional (requisitos organi-

zacionais, frequência, cronogramas, funções, tratamento de incidentes e dados). Inclui também a elaboração da estratégia de comunicação entre equipas e a especificação dos tipos e extensão dos testes técnicos e não técnicos a realizar, juntamente com os requisitos de documentação. O seu objetivo é assegurar uma abordagem estruturada, alinhada e eficaz para o processo de auditoria;
  - Considerações Legais: Este aspeto aborda a avaliação dos aspetos legais e regulamentares que podem impactar a auditoria. É crucial para garantir que todo o processo é conduzido em conformidade com a legislação aplicável (como o RGPD) e as obrigações contratuais, assegurando uma auditoria ética e dentro dos limites da lei.

- Avaliação dos Controlos de Segurança
  - Revisão dos controlos e procedimentos: Esta revisão abrange a análise do que a organização definiu como os seus controlos e políticas de segurança. O seu objetivo é verificar se a estratégia de proteção documentada está bem estruturada e é suficiente para os objetivos da empresa;
  - Avaliação dos controlos técnicos: Esta avaliação verifica na prática como os controlos estão a ser implementados e a funcionar. O seu propósito é garantir que as medidas de segurança adotadas estão a operar corretamente e a proteger a organização de forma eficaz.

- Recolha de Informações e Identificação de Ativos
  - *Footprinting* digital: Este processo abrange a recolha de informações públicas sobre a organização para identificar potenciais vulnerabilidades;
  - Descoberta da Rede: Esta etapa envolve a identificação de dispositivos e a análise da comunicação entre os dispositivos da rede;
  - Enumeração da Rede e Serviços: Explica a deteção de portos abertos e serviços em execução para avaliar riscos;
  - Análise de Vulnerabilidades: Descreve a identificação de pontos fracos nos sistemas e redes da organização.

- Identificação e Avaliação de Riscos
  - Conceitos de Risco: Esta fase inicial estabelece a base conceptual da auditoria. O seu foco é definir os conceitos de risco, ameaça e vulnerabilidade, para garantir uma linguagem e compreensão partilhadas ao longo de todo o processo;
  - Testes de Segurança de Credenciais: Nesta etapa, o foco é a segurança das 'chaves de acesso' da organização. São abordados os testes à robustez das palavras-passe e à proteção contra técnicas comuns de interceção, com o objetivo de avaliar a eficácia das políticas de autenticação;
  - Testes de Engenharia Social: Esta secção da auditoria aborda o fator humano da segurança. Explica como são simulados cenários de manipulação (como

emails de *phishing*) para avaliar a consciencialização e a capacidade de resposta da equipa a este tipo de ameaça;
  - Verificação de Vulnerabilidades de Sistemas e Aplicações: Abrange a verificação de sistemas e aplicações em busca de vulnerabilidades conhecidas e erros de configuração, com o propósito de mapear a superfície de ataque da organização;
  - Teste de Penetração: Após a identificação das vulnerabilidades, esta fase aborda a sua validação prática. Consiste na simulação de um ataque real para demonstrar o impacto que uma exploração bem-sucedida teria e o nível de acesso que um atacante poderia obter;
  - Classificação e Priorização de Riscos: Neste ponto, detalha-se o processo de organização das descobertas. Os riscos identificados são classificados com base no seu impacto e probabilidade, resultando numa priorização estratégica que permite focar os recursos nas ameaças mais significativas;
  - Plano de Mitigação e Recomendações: A fase final da auditoria foca-se na apresentação de soluções. Para cada risco, são detalhadas recomendações práticas e concretas, abrangendo as medidas técnicas e operacionais necessárias para a sua mitigação e para o fortalecimento da segurança.

- Resultados e Recomendações

  - Relatório de Auditoria: Esta secção final detalha o conteúdo e a estrutura do relatório de auditoria. O seu propósito é consolidar todas as análises e descobertas numa visão clara e abrangente da postura de segurança da organização, focando-se na apresentação de recomendações práticas e acionáveis para a mitigação dos riscos;
  - Melhoria Contínua: O roteiro conclui ao destacar a segurança como um processo contínuo, e não como um esforço único. Explica a importância de avaliar e adaptar constantemente as defesas em resposta a novas ameaças e vulnerabilidades, garantindo que a postura de segurança da organização se mantém robusta e eficaz ao longo do tempo.

5.2 Manual do Auditor

Nesta fase (Figura 5.11) do processo, procura-se estruturar e definir as componentes essenciais para garantir a eficácia e consistência das auditorias. Este processo envolve a definição de metodologias, critérios e procedimentos específicos que orientam cada fase da auditoria, proporcionando aos auditores uma abordagem clara e sistemática. A estrutura delineada tem como objetivo melhorar a eficácia das auditorias, facilitar a identificação de riscos e assegurar a normalização das práticas na organização auditada.

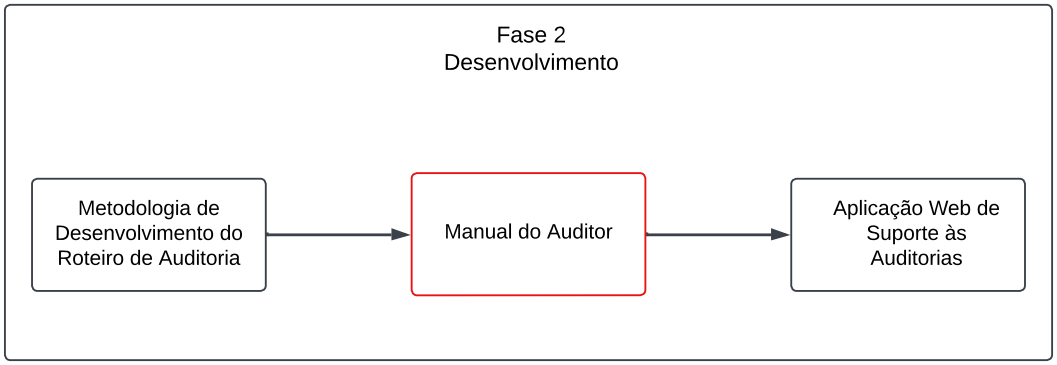

Figura 5.11: *Desenvolvimento do Manual do Auditor - Fase 2*

Objetivos do Manual do Auditor

O objetivo do Manual do Auditor é fornecer uma *framework* estruturada para a realização de auditorias de segurança, garantindo que estas são conduzidas de forma consistente, rigorosa e de acordo com as melhores práticas da indústria. O manual estabelece diretrizes claras para a realização de auditorias, o que contribui para a normalização dos processos e garante que a recolha e a análise de informações sejam realizadas de forma metódica e imparcial.

Este documento serve de guia de referência para os auditores, definindo metodologias, critérios de avaliação e procedimentos a adotar em cada fase da auditoria. Inclui os princípios básicos da auditoria de segurança, técnicas de recolha de provas, critérios de análise e parâmetros de identificação de riscos. Permite ainda que os auditores compreendam o contexto da organização auditada, os seus requisitos específicos e os objetivos da avaliação, garantindo que o processo é adaptado à realidade e às necessidades da entidade em questão.

Ao proporcionar uma abordagem estruturada, o manual melhora a fiabilidade e a reprodutibilidade das auditorias, reduzindo a subjetividade na interpretação dos resultados e aumentando a credibilidade das recomendações apresentadas. A normalização dos procedimentos também facilita a comparação entre auditorias, permitindo acompanhar a evolução da segurança da organização ao longo do tempo.

O manual do auditor não só apoia as auditorias, como também reforça a segurança das organizações de forma contínua. Ajuda a identificar pontos fracos nos processos e controlos de segurança e a implementar melhorias. Abrange aspetos técnicos e organizacionais, fornecendo uma avaliação abrangente da segurança da informação e da capacidade da organização para lidar com potenciais ameaças.

Estrutura do Manual do Auditor

De seguida, apresenta-se a estrutura do manual do auditor:

Planeamento e Preparação:

- Questionário Pré-Auditoria: Descreve o formulário enviado ao cliente antes da auditoria para recolher informações essenciais sobre âmbito, exclusões, logística e pontos de contacto;
- Desenvolvimento do Plano de Auditoria:

1. Define os objetivos, o âmbito e a logística da auditoria, para assegurar uma abordagem estruturada e eficaz;
2. A frequência da auditoria é definida com base nos objetivos da organização e na sua natureza (pontual ou recorrente), sendo ajustada conforme critérios como a criticidade dos ativos, as alterações tecnológicas e os requisitos regulamentares;
3. O calendário da auditoria (datas, objetivos intermédios e reuniões), a sua localização (presencial, remota ou mista, com os acessos necessários) e os equipamentos essenciais a utilizar para a realização dos testes também são especificados;
4. A definição clara das funções e responsabilidades de todos os intervenientes, tanto da equipa auditora quanto da organização cliente é detalhada, incluindo a atribuição de papéis, a identificação dos indivíduos e as autorizações necessárias;
5. O plano também define o Tratamento e Resposta a Incidentes, um procedimento padrão derivado do NIST SP 800-61 [57], que fornece uma abordagem estruturada e eficiente para a gestão de incidentes de segurança. Este procedimento destina-se especificamente a ser utilizado quando ocorre um incidente durante a auditoria e inclui as fases de preparação, deteção, análise, contenção, erradicação, recuperação e atividades pós-incidente. O principal objetivo é minimizar o impacto dos incidentes e melhorar a capacidade da organização para responder a futuros eventos, garantindo a continuidade do negócio e o cumprimento dos requisitos legais e regulamentares;
6. O plano define o processo para o Tratamento de Dados, alinhado com o Controlo 3 do CIS Controls [20], 'Proteção de Dados'. O processo inclui a definição clara dos responsáveis pela proteção dos dados, o tratamento adequado dos mesmos, como o armazenamento seguro, o acesso controlado, a transmissão e o processamento, bem como a implementação de medidas de segurança como cifragem de dados sensíveis e eliminação segura. A gestão de dados também aborda a conformidade com regulamentos como o RGPD, que exige a identificação dos responsáveis pelo tratamento, a finalidade, as categorias de dados e os prazos de retenção. Um dos principais objetivos é garantir a segurança e a confidencialidade dos dados, além de assegurar que, quando necessário, a destruição de dados seja realizada de forma irreversível e em conformidade com os requisitos legais e regulamentares;
7. A estratégia de comunicação define os canais e métodos para a interação entre a equipa de auditoria e a organização, visando assegurar uma colabo-

ração transparente e eficaz ao longo de todo o processo;

8. A execução dos testes abrange a identificação e avaliação dos controlos a serem avaliados, bem como a realização dos testes técnicos necessários para verificar a eficácia das medidas de segurança;
9. Por fim, as considerações legais referem-se à avaliação dos aspetos legais e regulamentares que podem impactar a auditoria, sendo crucial para garantir que todo o processo é conduzido em total conformidade.

Avaliação dos Controlos de Segurança:

- Verificação dos Controlos de Segurança: Avalia as medidas implementadas face às categorias do QNRCS (Identificar, Proteger, Detetar, Responder) para proteger os ativos;
- Análise de Controlos Técnicos, Físicos e Administrativos: Abrange a análise de controlos essenciais como a classificação de ativos, segurança física (controlo de acessos), monitorização/deteção de eventos de segurança e os processos de resposta a incidentes;
- Revisão de Políticas de Segurança: Descreve a verificação de políticas como a de segurança da informação, gestão de senhas e gestão de fornecedores, para garantir o alinhamento com os controlos;
- Processo de Auditoria com a Aplicação Web: Descreve o processo completo da auditoria, desde o acesso do cliente à aplicação web para o preenchimento do questionário sobre a implementação dos controlos, até à revisão e validação das respostas.

Recolha de Informações e Identificação de Ativos:

- *Footprinting* digital: Detalha a recolha passiva de informações públicas (domínios, IPs, emails, funcionários, tecnologias, fugas de dados) através de ferramentas automatizadas (SpiderFoot[1]), pesquisa avançada (Google Dorks[2]) e análise de fontes online (WHOIS, Shodan[3], HIBP[4], Netcraft[5], etc.);
- Descoberta da Rede: Abrange a descoberta passiva (*sniffing* de tráfego com Wireshark[6]/Kismet[7] para análise de protocolos e dados em redes com/sem fios) e ativa (identificação de *hosts* ativos na rede com Nmap[8]/Zenmap[9]);
- Identificação de Portos e Serviços: Descreve a identificação de portos abertas (`nmap -sSU`), a determinação de serviços/versões (`nmap -sV`) e sistemas operativos (`nmap -O`), e a enumeração detalhada de configurações via *scripts* do Nmap;

[1] Descrição e URL da ferramenta SpiderFoot no Apêndice C.
[2] Descrição de Google Dorks no Apêndice C.
[3] Descrição e URL da ferramenta Shodan no Apêndice C.
[4] Descrição e URL da ferramenta HIBP no Apêndice C.
[5] Descrição e URL da ferramenta Netcraft no Apêndice C.
[6] Descrição e URL da ferramenta Wireshark no Apêndice C.
[7] Descrição e URL da ferramenta Kismet Wireless no Apêndice C.
[8] Descrição e URL da ferramenta Nmap no Apêndice C.
[9] Descrição e URL da ferramenta Zenmap no Apêndice C.

- Análise de Vulnerabilidades: Detalha a utilização de *scanners* (Nessus[10], Nmap 'vuln'/'vulners', Nikto[11], WhatWeb[12]) e análise manual para identificar vulnerabilidades conhecidas nos serviços e aplicações detetados, para preparar a fase de testes de penetração.

Identificação e Avaliação de Riscos:

- Testes de Segurança de Credenciais: Este item abrange a avaliação da robustez das credenciais e a proteção contra técnicas comuns de interceção, como ataques *Man-in-the-Middle* (MitM) utilizando ferramentas como o Bettercap[13] e o Responder[14], bem como *password cracking* com ferramentas como o Hashcat[15];
- Testes de Penetração no Local: Esta secção foca-se na avaliação dos controlos de acesso às instalações e na identificação de vulnerabilidades físicas na organização;
- Testes de Engenharia Social: Esta área explora a avaliação das vulnerabilidades humanas através de técnicas como *phishing*, frequentemente com o apoio de ferramentas como o GoPhish[16];
- Verificação de Vulnerabilidades de Sistemas e Aplicações: Este tópico engloba a análise de segurança de aplicações, incluindo Testes de Segurança Estáticos (SAST) com ferramentas como o SonarQube[17], e Dinâmicos (DAST) através de ferramentas como o Zaproxy[18] e o Burp Suite[19]. Também abrange a auditoria de configurações de sistemas, por exemplo, com o Wazuh[20] em conformidade com CIS *benchmarks* [58], para identificar pontos fracos;
- Testes de Penetração e Exploração: Esta etapa descreve a simulação de ataques reais e a exploração de vulnerabilidades identificadas, utilizando ferramentas como o Metasploit[21], para avaliar a postura de segurança da organização;
- Classificação e Priorização de Riscos: Esta fase detalha a classificação de riscos, baseando-se em métricas como CVSS (impacto) e EPSS (probabilidade). Inclui a subsequente priorização para mitigação, considerando o nível de risco calculado e o contexto organizacional (por exemplo, criticidade do sistema, exposição, tolerância ao risco);
- Mitigação e Recomendações: Este item descreve as ações para mitigar vulnerabilidades, como a aplicação de *patches*, a atualização de controlos e a implemen-

[10] Descrição e URL da ferramenta Nessus no Apêndice C.
[11] Descrição e URL da ferramenta Nikto no Apêndice C.
[12] Descrição e URL da ferramenta WhatWeb no Apêndice C.
[13] Descrição e URL da ferramenta Bettercap no Apêndice C.
[14] Descrição e URL da ferramenta Responder no Apêndice C.
[15] Descrição e URL da ferramenta Hashcat no Apêndice C.
[16] Descrição e URL da ferramenta GoPhish no Apêndice C.
[17] Descrição e URL da ferramenta SonarQube no Apêndice C.
[18] Descrição e URL da ferramenta Zaproxy no Apêndice C.
[19] Descrição e URL da ferramenta Burp Suite no Apêndice C.
[20] Descrição e URL da ferramenta Wazuh no Apêndice C.
[21] Descrição e URL da ferramenta Metasploit Framework no Apêndice C.

tação de novas tecnologias. Inclui a abordagem estruturada para a remediação, envolvendo testes, coordenação entre equipas e verificação da eficácia.

Resultados e Recomendações:

- Relatório de Auditoria: Descreve a estrutura do relatório final, que inclui um resumo executivo com as principais descobertas, a visão geral e âmbito da auditoria, um sumário das vulnerabilidades e riscos identificados com a sua classificação, o detalhe técnico dos resultados dos testes, as recomendações de mitigação e uma avaliação geral da segurança da organização;

Apêndices

- Testes de Penetração e Pós-Exploração: Este apêndice detalha exemplos de procedimentos para a execução destas atividades. Inclui métodos para a exploração de serviços com credenciais obtidas, exemplos de testes de penetração com ferramentas específicas, e técnicas de pós-exploração como quebra de *passwords* e persistência;
- Manual de Instalação de Ferramentas: Este apêndice detalha os procedimentos e requisitos para a instalação das ferramentas de cibersegurança utilizadas na auditoria;
- Cálculos e Metodologias de Risco: Este apêndice apresenta as metodologias detalhadas para a avaliação da criticidade e exposição ao risco. Abrange o cálculo da pontuação total de exposição, a percentagem de risco, o sistema de classificação de risco por atividade de auditoria e o cálculo para a avaliação final da empresa, com os seus pesos e interpretações.

5.2.1 Estrutura de Cada Fase da Auditoria

De seguida, apresenta-se a estrutura de cada fase da auditoria:

- Objetivo: Descrever o propósito da atividade, especificando o que se pretende alcançar e a sua relevância no contexto da análise.
- Procedimento: Indicar os passos a seguir para realizar a atividade, garantindo que a execução seja eficaz e reproduzível. Detalha a execução, abordando a sequência exata de ações e a interação entre diferentes componentes.
- Utilização das Ferramentas: Especificar os recursos necessários para a atividade, incluindo software, hardware, ou outras ferramentas. Para cada ferramenta mencionada, o manual detalha a finalidade, as funcionalidades relevantes e os parâmetros essenciais para uma configuração correta. Quando aplicável, são apresentados exemplos de utilização para garantir a correta execução dos procedimentos. Caso existam restrições, como compatibilidade com determinados sistemas ou requisitos técnicos específicos, são assinaladas.

Cada fase da auditoria exigiu uma pesquisa detalhada e uma avaliação rigorosa das ferramentas a utilizar. As ferramentas selecionadas foram, então, testadas numa máquina virtual com Kali Linux[22]. Todos os comandos necessários para instalar as ferramentas foram registados, bem como os comandos utilizados para obter os resultados pretendidos. Este processo foi fundamental para garantir a funcionalidade e a eficácia das ferramentas no contexto da auditoria e permitiu uma análise mais exata e completa dos dados.

- Análise de Riscos: Os resultados dos testes realizados serão avaliados para determinar os possíveis riscos associados a cada atividade. A cada critério identificado será atribuído um Nível de Risco e o seu Peso Percentual correspondente, de acordo com a metodologia de classificação de risco já apresentada na Secção 5.1.3.
- Registo de Dados: O registo de dados deve assegurar que todas as informações relevantes sobre a atividade realizada são documentadas de forma estruturada e consistente. Inclui detalhes sobre os métodos aplicados, os parâmetros utilizados e os resultados obtidos, facilitando a análise, validação e consulta futura.

5.3 Aplicação Web de suporte às auditorias

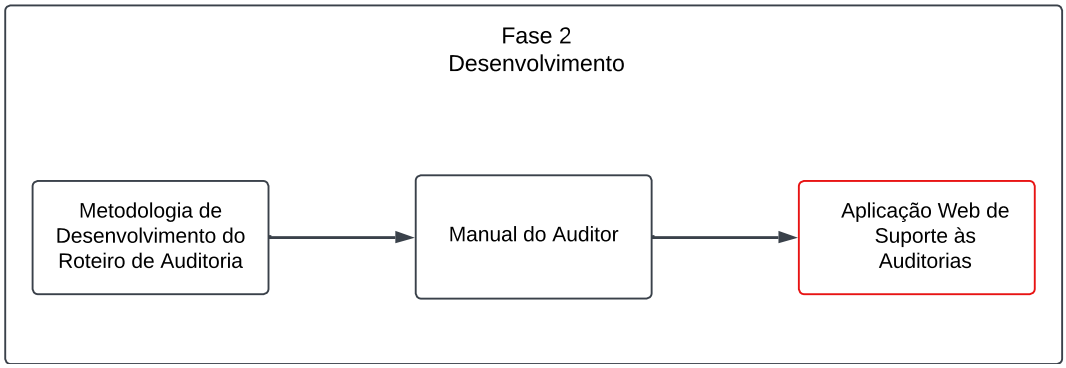

Figura 5.12: *Desenvolvimento Aplicação Web - Fase 2*

A metodologia de auditoria proposta neste trabalho envolve múltiplos processos e a recolha estruturada de informação, incluindo a classificação de risco por atividade. Para facilitar a aplicação prática desta metodologia pelos auditores e fornecer uma interface clara para os clientes, tornou-se evidente a necessidade de desenvolver uma aplicação web de suporte.

Esta aplicação foi concebida como uma plataforma centralizada, cujo propósito principal é guiar o auditor em todas as fases da auditoria. A sua estrutura facilita o registo sistemático de observações e avaliações de risco, além de organizar a informação recolhida para facilitar a consulta pelo cliente e a subsequente elaboração do relatório de auditoria. Desta forma, otimiza-se a gestão da informação da auditoria e padroniza-se a aplicação da metodologia.

[22]Descrição e URL da ferramenta Kali Linux no Apêndice C.

5.3.1 Definição de Requisitos Funcionais

O processo da definição dos requisitos funcionais da aplicação web baseou-se diretamente nas necessidades identificadas durante a concepção do manual de auditoria descrito anteriormente na Secção 5.2. A estrutura de avaliação de risco, comum a diversas fases da auditoria (conforme exemplificado na Estrutura de Cada Fase da Auditoria), evidenciou a necessidade de uma interface uniforme para o registo destas avaliações, incluindo a justificação associada, a identificação das ferramentas utilizadas, comandos executados e resultados obtidos. Esta abordagem representa uma melhoria significativa face à gestão de dados em folhas de cálculo ou documentos isolados. Adicionalmente, foram analisadas plataformas de auditoria existentes para identificar boas práticas e funcionalidades relevantes, como a visão geral do estado da segurança e a classificação de vulnerabilidades.

Os requisitos funcionais essenciais foram definidos em reunião conjunta com a equipa de desenvolvimento. Estes requisitos serviram como o "caderno de encargos"para a implementação e incluem, entre outros:

- **Gestão de Utilizadores e Perfis:** Criação e gestão de contas distintas para Clientes, Auditores e Administradores, cada um com permissões específicas;
- **Gestão de Modelos de Formulários e Auditorias:** Permite que administradores e auditores criem, personalizem e mantenham uma variedade de modelos de formulários essenciais totalmente adaptáveis a diferentes âmbitos e contextos, incluindo:
  - Planos de Auditoria de Segurança;
  - Formulários para Recolha de Informação e Ativos;
  - Formulários de Identificação e Avaliação de Riscos;
  - Questionários Pré-auditoria;
  - Formulários para Avaliação de Controles de clientes.

  Esta funcionalidade otimiza a padronização e a eficiência dos processos de auditoria, incluindo a capacidade de associar e ajustar pesos específicos aos critérios de avaliação. O sistema também suporta a atribuição de auditorias a clientes e auditores específicos.
- **Interface do Auditor:** Permite ao auditor selecionar um formulário e preencher os dados da auditoria seguindo o modelo definido. Permite ainda visualizar o estado das auditorias ativas e do progresso do cliente (no preenchimento do seu formulário, se aplicável), e inclui funcionalidade para submeter e finalizar a auditoria. Para cada auditoria, a aplicação também apresenta uma visão consolidada dos achados mais relevantes, classificados por nível de risco e com a indicação da quantidade de ocorrências por cada categoria;
- **Interface do Cliente:** Permite ao cliente interagir e colaborar no processo de auditoria, através do preenchimento de questionários de pré-auditoria e de controlos de segurança (quando aplicável). No questionário, para cada controlo, o

cliente seleciona entre as opções: "Totalmente Implementado", "Parcialmente Implementado", "Pouco Implementado"ou "Nada Implementado". Se um controlo não estiver "Totalmente Implementado", é solicitado um breve esclarecimento sobre a situação atual, planos futuros ou dificuldades, através de uma área de texto com a instrução. Após a conclusão da auditoria, a interface apresenta as métricas gerais de avaliação da segurança. Além disso, para cada auditoria, o cliente tem acesso a uma visão consolidada dos achados mais relevantes, incluindo lacunas na implementação de controlos, classificados por nível de risco e com a indicação da quantidade de ocorrências por cada categoria, facilitando a priorização e o planeamento das ações de remediação;

- **Visualização de Dados e Vulnerabilidades:** Apresentação gráfica (ex: gráficos circulares, cartões sumários coloridos) da classificação de risco geral e por atividade. Listagem e classificação de vulnerabilidades identificadas por nível de risco (ex: Informativo, Baixo, Moderado, Elevado, Crítico), probabilidade, de forma a apoiar o cliente na priorização das ações de remediação.

5.3.2 Implementação Técnica

A fase de programação e desenvolvimento técnico da aplicação web foi realizada dentro da empresa, utilizando as tecnologias PHP [59] e a *framework* Laravel [60] (Figura 5.13). O desenvolvimento procurou seguir as especificações funcionais definidas na reunião de requisitos mencionada anteriormente.

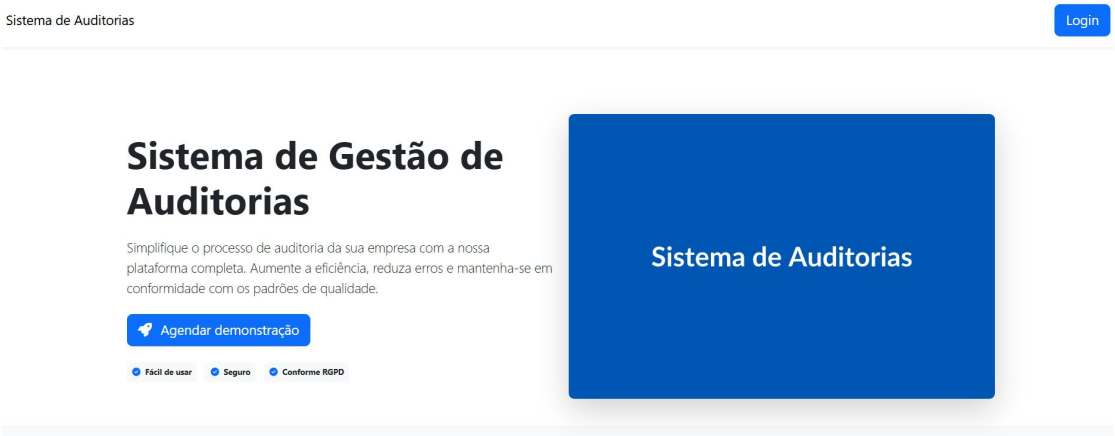

Figura 5.13: *Plataforma Web*

5.3.3 Validação e Teste

Após a implementação das funcionalidades, iniciou-se o processo de validação. Este processo teve como objetivo principal garantir a conformidade da aplicação com os requisitos funcionais especificados e assegurar a sua adequação aos objetivos do projeto. Foram realizados os seguintes tipos de testes manuais:

- Testes Funcionais: Verificação sistemática de cada funcionalidade implementada,

comparando o seu comportamento com o esperado de acordo com os requisitos definidos;
- Testes de Usabilidade: Avaliação da facilidade de uso das interfaces, clareza da navegação e da apresentação da informação, tanto na perspetiva do auditor como do cliente;
- Testes de Aceitação: Validação global da aplicação face aos objetivos definidos, simulando cenários de utilização completos.

Para verificar a correspondência da implementação com as especificações, foram simulados os principais fluxos de utilização. Um exemplo de cenário testado incluiu:

1. Criação de contas (auditor, cliente, admin);
2. Criação de um formulário de auditoria e de um formulário de controlos pelo admin;
3. Criação de uma nova auditoria, associando cliente, auditores e os respetivos formulários;
4. Acesso do cliente para visualização e preenchimento do formulário de controlos;
5. Acesso do auditor para verificar o progresso do cliente e preencher o formulário de auditoria;
6. Finalização da auditoria pelo auditor;
7. Visualização dos resultados consolidados, métricas e vulnerabilidades pelo cliente;

Durante esta fase de validação, foram identificados alguns aspetos a melhorar, como erros de redirecionamento e pormenores da interface em falta. Adicionalmente, os testes levaram a refinamentos nos pesos utilizados nas avaliações e na forma como algumas métricas eram calculadas. O processo foi estruturado de forma iterativa, em que os problemas identificados eram reportados à equipa de desenvolvimento para correção, seguindo-se um novo ciclo de testes de validação.

Após a conclusão do processo de validação, a aplicação *web* encontra-se plenamente funcional e pronta para utilização. Esta plataforma não só permite uma visualização clara das métricas e resultados da auditoria, como se destaca pela sua flexibilidade na criação e modificação de formulários. Tal capacidade assegura que os modelos de auditoria possam ser totalmente adaptados e personalizados para cada tipo de auditoria e para as necessidades específicas de cada cliente.

6
Caso de Estudo

Este capítulo tem como objetivo principal apresentar a aplicação e validação prática da metodologia de auditoria e da aplicação *web* de suporte, concretizando os princípios delineados na Fase 3 - Validação (Figura 6.1). Para o efeito, recorre-se a um caso de estudo detalhado que, ao simular o ciclo de vida completo de uma auditoria, permite aferir a validade e a eficácia da estrutura metodológica proposta como instrumento de avaliação da maturidade de cibersegurança de uma organização.

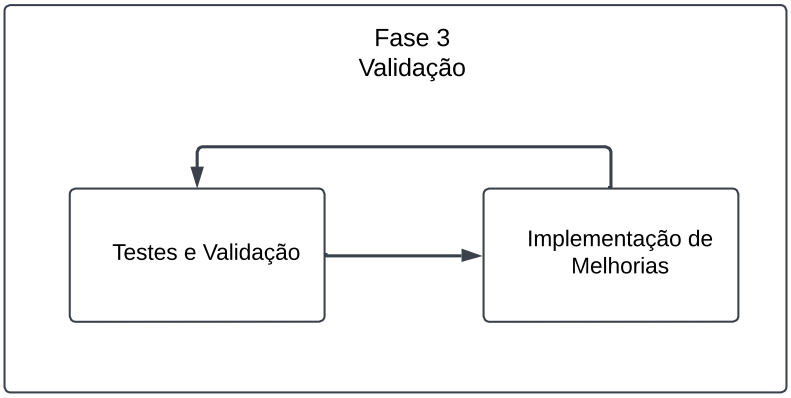

Figura 6.1: *Validação - Fase 3*

6.1 Descrição do Cenário de Aplicação

O caso de estudo foi conduzido numa PME do setor de tecnologias de informação, denominada "Empresa A"para fins de confidencialidade. Esta organização, embora possua uma infraestrutura de TI já desenvolvida, apresenta um desafio significativo no que toca à sua cibersegurança, que se encontra em fase de formalização e otimização. Este perfil torna-a um cenário ideal para a validação da abordagem proposta.

O objetivo principal desta auditoria foi, por um lado, avaliar a postura de segurança atual da Empresa A face aos controlos definidos na metodologia e, por outro, validar a eficácia da metodologia desenvolvida na orientação do processo de auditoria e na

consolidação de resultados claros e acionáveis.

6.2 Execução da Metodologia de Auditoria

A auditoria à Empresa A seguiu rigorosamente as fases da metodologia detalhada no Capítulo 5. A aplicação *web* desempenhou um papel central em todas as etapas, desde a preparação inicial até à criação de relatórios.

Os passos realizados durante este caso de estudo, com o apoio da aplicação, são detalhados nas subsecções seguintes.

6.2.1 Configuração Inicial

O administrador da plataforma criou as contas de utilizador para o auditor e para um representante da Empresa A. A etapa subsequente consistiu na configuração da auditoria na plataforma, através da atribuição de formulários específicos a cada interveniente. Ao cliente, foram atribuídos o "Questionário Pré-Auditoria"e o formulário de "Avaliação de Controlos". Enquanto que, ao auditor foram atribuídos os formulários de "Plano de Auditoria de Segurança", "Recolha de Informações e Identificação de Ativos"e "Identificação e Avaliação de Riscos". Um exemplo desta configuração é apresentado na Figura 6.2. Este processo evidencia a flexibilidade da aplicação, que permite ajustar o fluxo de trabalho e os instrumentos de recolha de dados às necessidades do cenário da Empresa A, demonstrando a sua capacidade de personalização.

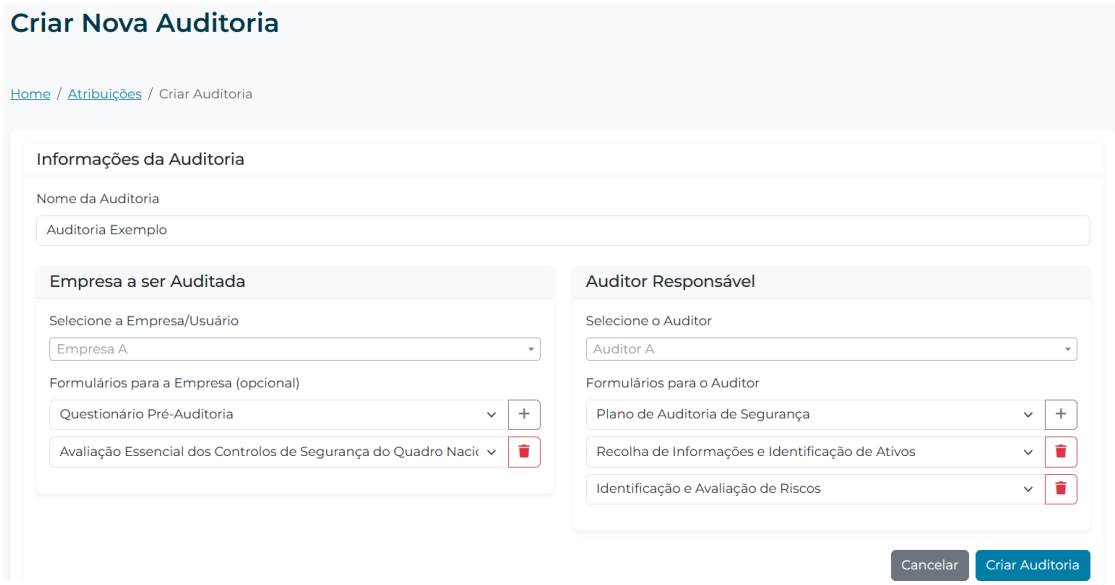

Figura 6.2: *Configuração da Auditoria: Atribuição de Formulários e Responsáveis*

6.2.2 Início da Auditoria

Com a configuração concluída, a auditoria foi iniciada na plataforma, disponibilizando os formulários atribuídos a cada interveniente (Figura 6.3 e Figura 6.4).

Figura 6.3: *Visualização dos formulários pendentes na interface do cliente*

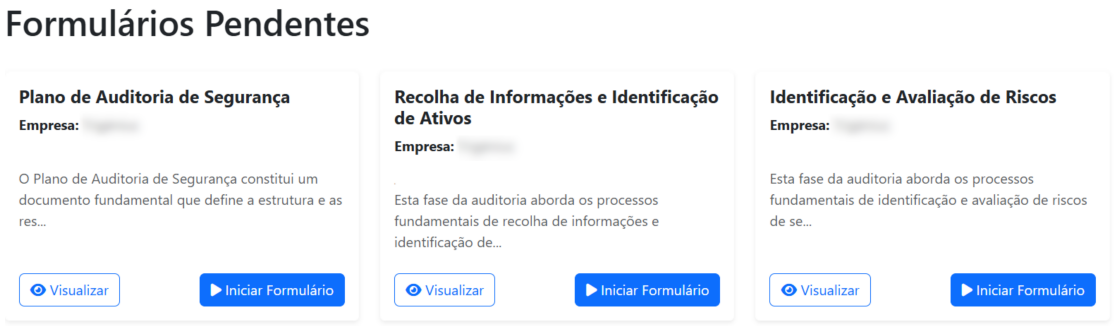

Figura 6.4: *Visualização dos formulários pendentes na interface do auditor*

6.2.3 Definição do Âmbito e Planeamento Inicial

O processo iniciou-se com o acesso do representante da Empresa A à plataforma, onde preencheu o "Questionário Pré-Auditoria"(Figura 6.5) para fornecer informações cruciais sobre o âmbito, exclusões e logística. Com base nestes dados preliminares e nas informações recolhidas numa reunião subsequente com o cliente, o auditor utilizou a plataforma para elaborar o "Plano de Auditoria". Este documento consolidou os objetivos, o âmbito definitivo e as áreas de foco principais, servindo como guia para as etapas seguintes.

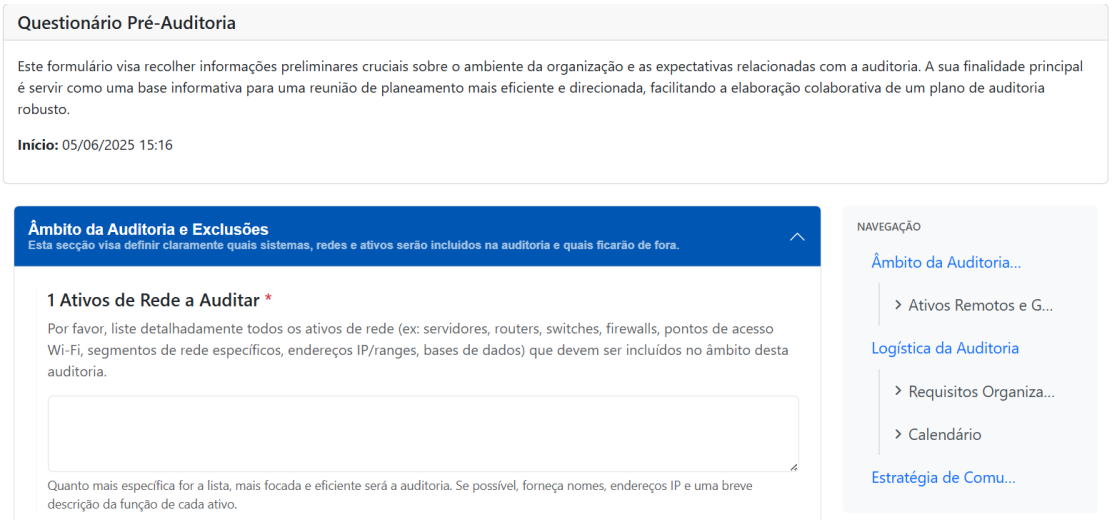

Figura 6.5: *Interface do Questionário Pré-Auditoria*

6.2.4 Preenchimento do Formulário de Controlos

Após a definição do plano, o cliente procede ao preenchimento do 'Formulário de Avaliação de Controlos' na aplicação. A Figura 6.6 ilustra exemplos das questões apresentadas e as opções de resposta para avaliação da conformidade. Nesta fase, o representante da Empresa A indicou o nível de conformidade e forneceu observações sobre cada controlo de segurança, criando um registo detalhado que seria posteriormente validado e aprofundado na análise do auditor. O resultado consolidado desta avaliação, incluindo a exposição ao risco e o estado de segurança, é exemplificado na Figura 6.7.

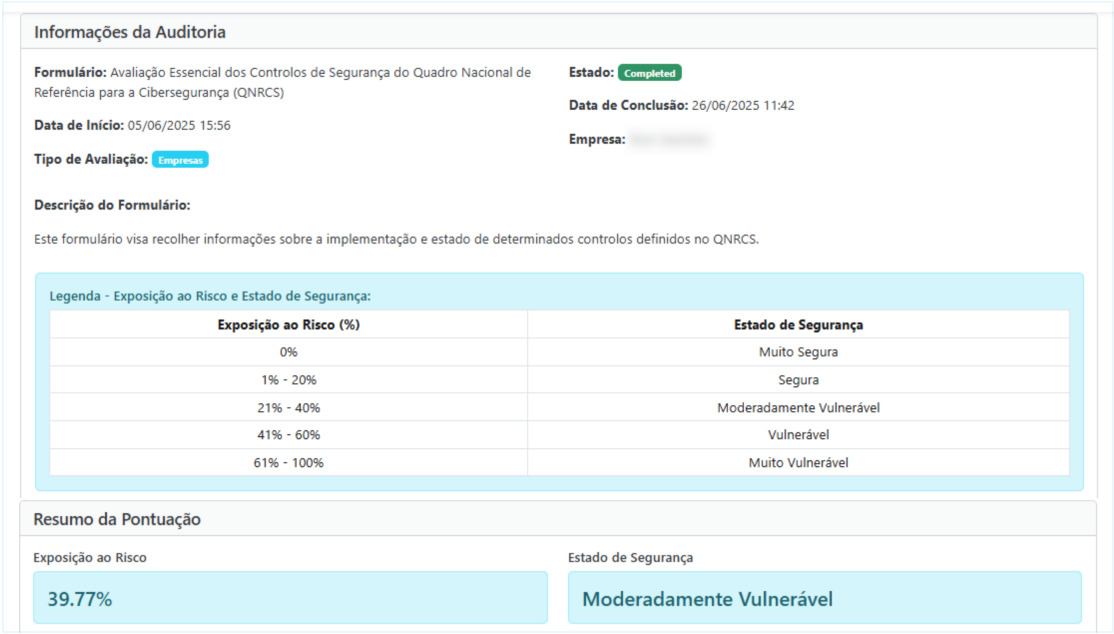

Figura 6.7: *Resultados da Avaliação de Controlos: Exposição ao Risco e Estado de Segurança*

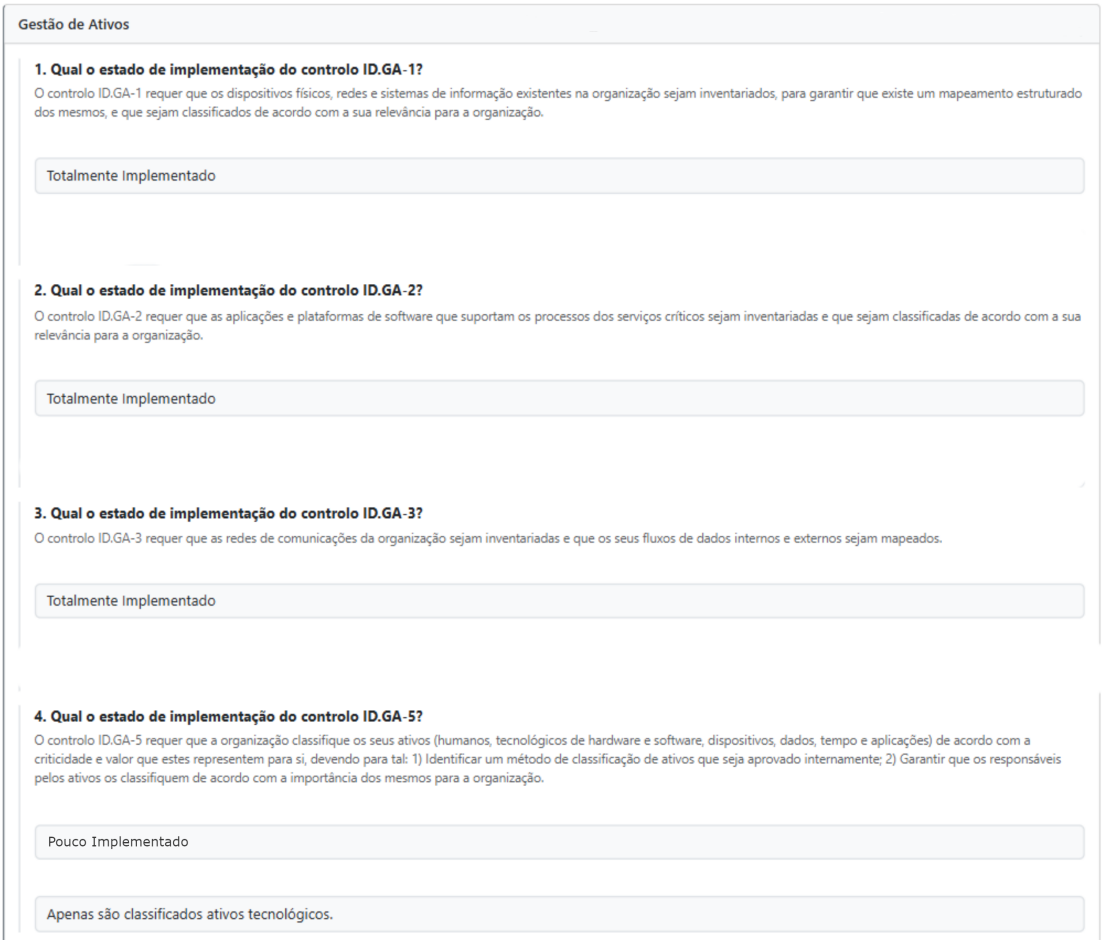

Figura 6.6: *Formulário de Avaliação de Controlos de Segurança* (*Gestão de Ativos*)

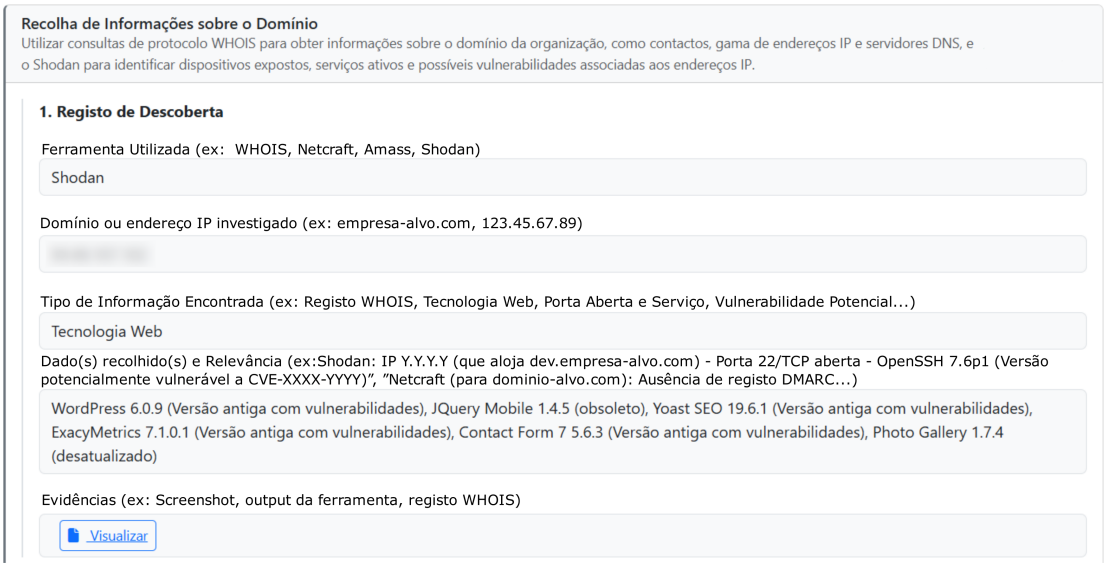

Figura 6.8: *Registo de Descoberta Relativa ao Domínio*

6.2.5 Levantamento de Ativos e Análise de Riscos

Nesta etapa, o auditor realizou um processo de análise em duas fases. Primeiro, no formulário de "Recolha de Informações e Identificação de Ativos", procedeu ao levantamento da infraestrutura e ao mapeamento de potenciais pontos de entrada e vulnerabilidades. Um exemplo do registo de descobertas de ativos e vulnerabilidades é ilustrado na Figura 6.8. A pontuação de risco resultante desta primeira fase é apresentada na Figura 6.9. Posteriormente, no formulário de "Identificação e Avaliação de Riscos", o auditor aprofundou a análise, validando as vulnerabilidades previamente mapeadas e identificando outras através de uma investigação mais exaustiva, classificando as ameaças e quantificando o risco. O resultado final desta avaliação de risco é visualizado na Figura 6.10. Este método de duas fases culminou na elaboração de um perfil de risco preciso e acionável, que dá prioridade às ameaças que representam o risco mais significativo para a organização.

6.2.6 Conclusão e Apresentação dos Resultados

A última etapa do processo consistiu na conclusão formal da auditoria pelo auditor na plataforma. O sistema, por sua vez, ficou responsável pelo processamento automático, que envolveu o cálculo das métricas e a consolidação de todos os dados e riscos identificados. Os resultados finais são disponibilizados em dois formatos: uma interface web interativa e um relatório detalhado para download. Um exemplo do resumo da pontuação final consolidada na interface web é apresentado na Figura 6.11. Juntos, estes elementos não só apresentam o estado atual da segurança, mas também priorizam os riscos para guiar as futuras atividades de remediação.

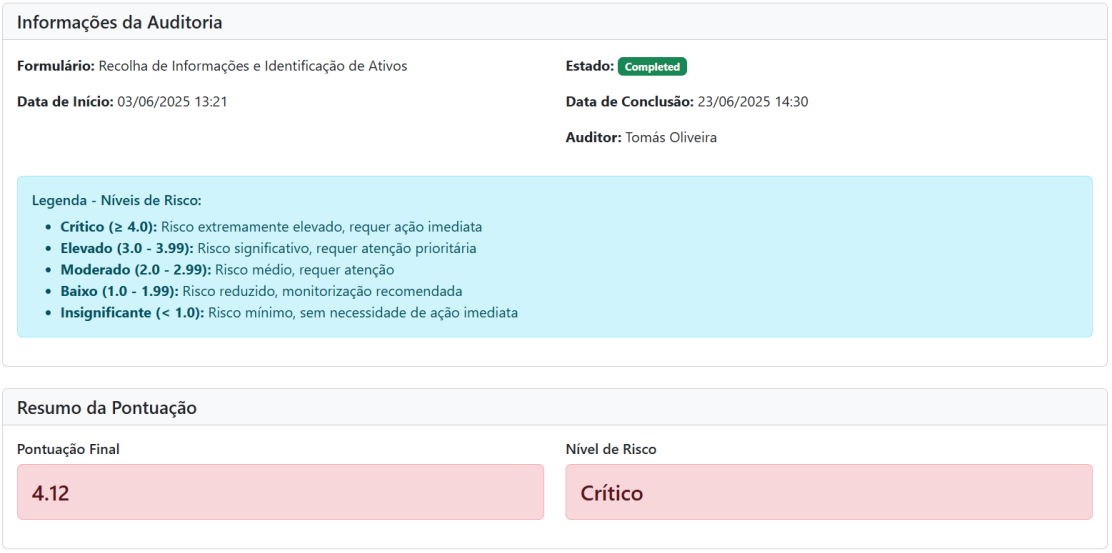

Figura 6.9: *Avaliação de Risco da Recolha de Informações e Identificação de Ativos*

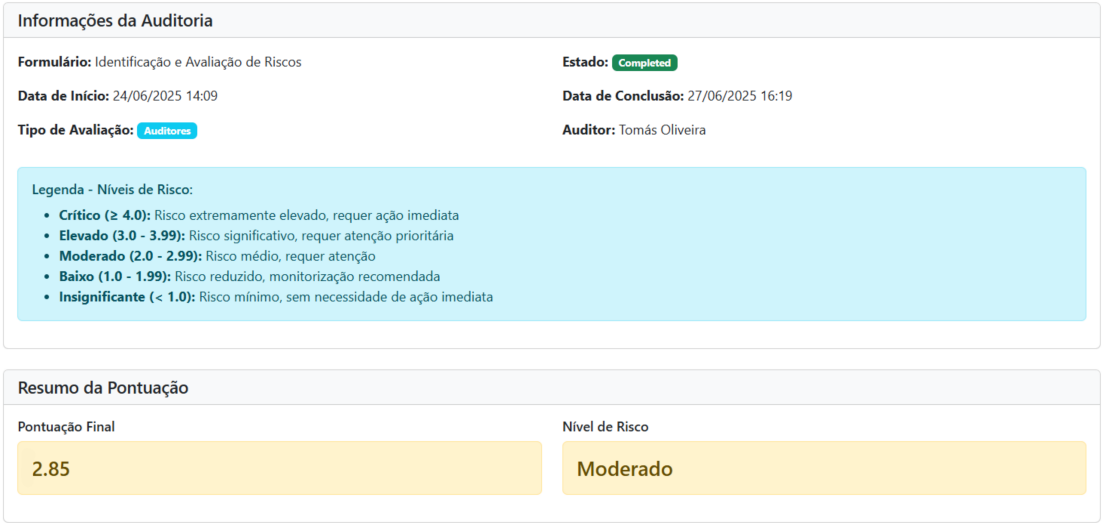

Figura 6.10: *Avaliação de Risco da Identificação e Avaliação de Riscos*

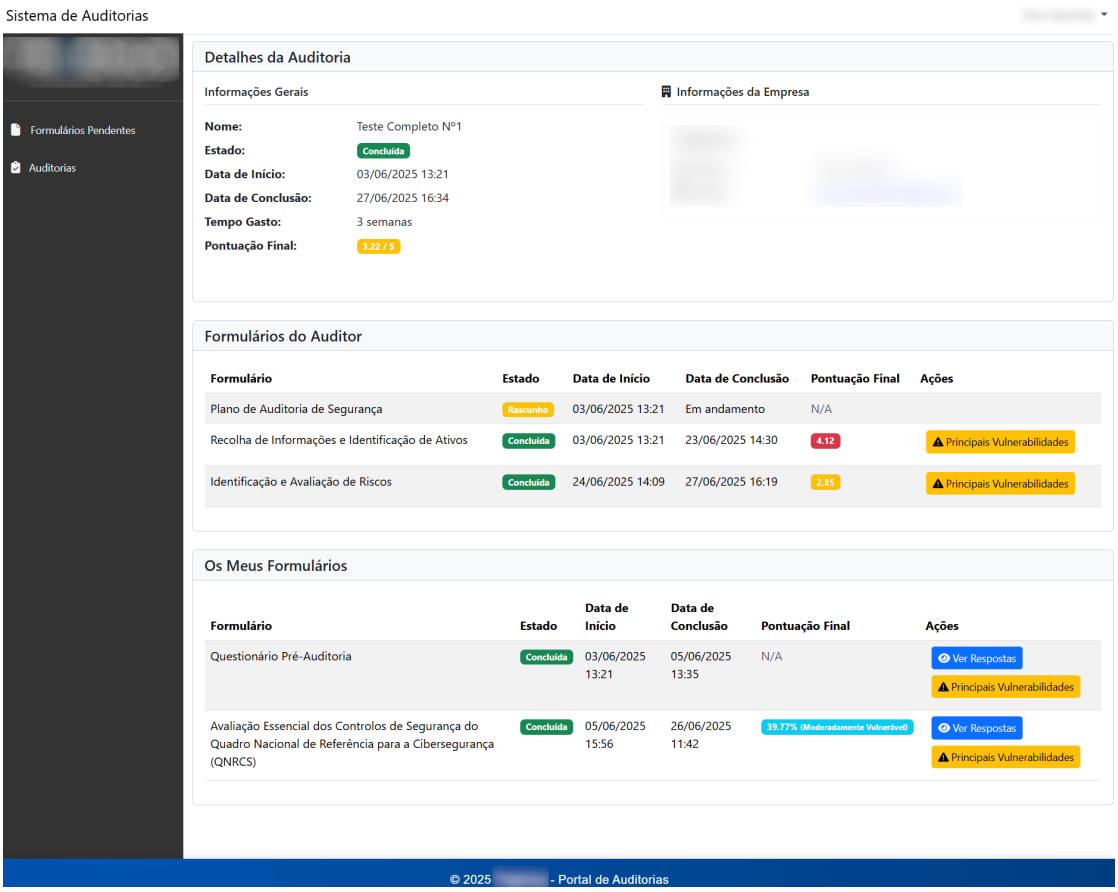

Figura 6.11: *Resumo da Pontuação de Risco Final na Interface Web*

6.3 Resultados e Análise

Os resultados da auditoria à Empresa A, gerados e visualizados através da aplicação web, forneceram uma análise quantitativa e qualitativa da sua postura de cibersegurança.

- **Métricas de Avaliação:** A aplicação apresentou de forma clara a Pontuação Global de Risco da Empresa A na Figura 6.10, bem como a Percentagem de Exposição ao Risco na Figura 6.7, indicando o seu nível de segurança atual como Moderadamente Vulnerável.
- **Análise e Visualização de Vulnerabilidades:** A plataforma lista e classifica as vulnerabilidades detetadas, apresentando-as de forma organizada por nível de risco. Conforme ilustrado na Figura 6.12, é fornecido um resumo visual dos riscos por categoria (Nenhum, Baixo, Médio, Grande, Crítico), juntamente com a contagem total de ocorrências. Esta representação visual, através de cartões sumários coloridos, permite ao cliente e ao auditor identificar rapidamente as áreas críticas que exigem atenção imediata e priorizar as ações de remediação.

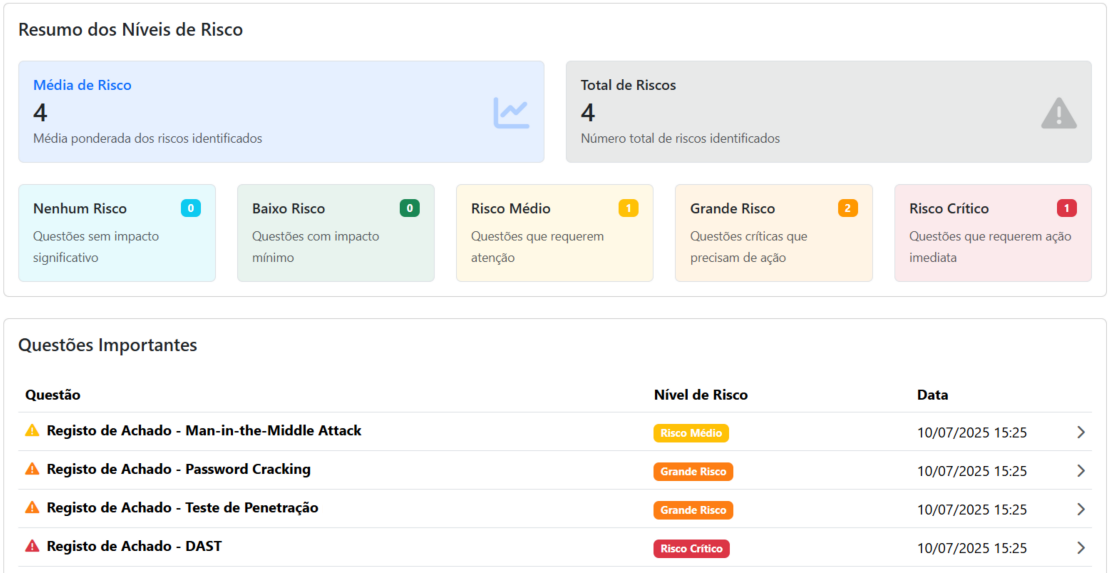

Figura 6.12: *Métricas e Resumo de Riscos na Aplicação Web*

- **Interface e Usabilidade:** A avaliação da usabilidade revelou que a interface da aplicação é clara e de fácil navegação, facilitando a interação tanto para o auditor, no registo de descobertas e avaliação de riscos, quanto para o cliente, no preenchimento de questionários e na visualização de relatórios. A flexibilidade do sistema, evidenciada pela capacidade de ajustar os pesos das avaliações e a forma de cálculo de algumas métricas durante a validação iterativa, demonstrou a robustez e adaptabilidade da aplicação aos refinamentos exigidos.

6.4 Refinamentos e Contribuições do Caso de Estudo

O caso de estudo realizado revelou-se fundamental para identificar oportunidades de melhoria, abrangendo tanto a metodologia descrita no manual quanto a funcionalidade da aplicação *web*.

Este processo permitiu refinar diretamente o manual de auditoria, otimizando a descrição de cada fase do processo, clarificando a utilização das ferramentas e promovendo uma maior objetividade e clareza na análise de risco. Consequentemente, estas revisões guiaram as atualizações nos formulários da plataforma e encontram-se já refletidas na especificação apresentada no Capítulo 5.

Especificamente, os formulários ”Questionário Pré-Auditoria”e ”Plano de Auditoria de Segurança”foram semanticamente ajustados para maior clareza. O formulário de ”Avaliação Essencial dos Controlos de Segurança QNRCS”foi objeto de uma revisão mais aprofundada, com a remoção de controlos menos críticos e a adição de outros mais pertinentes, garantindo uma avaliação mais focada e eficaz. O conteúdo das secções de ”Recolha de Informações e Identificação de Ativos”e ”Identificação e Avaliação de Riscos”foi refinado, juntamente com as orientações para o uso das ferramentas, o que resultou numa avaliação de risco mais detalhada e objetiva.

A interação prática com o sistema durante o caso de estudo permitiu ainda a identificação e correção de *bugs*, a implementação de funcionalidades de melhoria da experiência do utilizador e o reconhecimento de áreas para futuras otimizações do sistema.

6.5 Discussão e Conclusões do Caso de Estudo

A análise deste caso de estudo confirmou a viabilidade e a eficácia da metodologia de auditoria e da aplicação *web* no suporte a avaliações de cibersegurança. Foi demonstrada a clareza e abrangência do manual do auditor como guia para as etapas de execução e para os critérios de avaliação, e a capacidade da aplicação em facilitar a identificação e a classificação das vulnerabilidades. A relevância destas características revelou-se particularmente significativa em contextos como o da Empresa A, onde a cibersegurança se encontra em fase de formalização e otimização. A capacidade de personalizar os formulários e a estrutura da auditoria constituiu uma mais-valia, permitindo que a metodologia se adaptasse aos desafios e recursos específicos da empresa auditada, e evitando processos excessivamente burocráticos e dispendiosos.

A aplicação demonstrou ser uma ferramenta robusta para centralizar a recolha de dados, automatizar cálculos de risco e apresentar resultados de forma compreensível. Esta funcionalidade capacita tanto auditores quanto clientes a obter informações acionáveis sobre a postura de segurança, facilitando a priorização das ações de remediação e a tomada de decisões informadas, o que contribui para a melhoria contínua da segurança cibernética da organização. Em síntese, os resultado obtidos no caso de estudo reforçam o valor da aplicação, consolidando-a como um contributo essencial para a padronização e otimização dos processos de auditoria de cibersegurança, promovendo a sua acessibilidade e eficácia em diversos tipos de organizações.

7
Conclusões

No atual panorama digital, a cibersegurança deixou de ser uma preocupação exclusiva das grandes corporações para se tornar um pilar essencial à sobrevivência e confiança de qualquer organização. As Pequenas e Médias Empresas (PME), que constituem a grande maioria do tecido empresarial português, enfrentam desafios únicos, como a escassez de recursos financeiros e de conhecimento especializado, juntamente com a complexidade das normas e *frameworks* existentes, os quais criam uma barreira significativa à implementação de práticas de segurança robustas. Foi com o objetivo de colmatar esta lacuna que o presente projeto foi desenvolvido, com o intuito de criar uma estrutura de auditoria de cibersegurança prática, acessível e adaptada à realidade das PME.

Para atingir este fim, o trabalho foi estruturado em três pilares fundamentais e interdependentes, nomeadamente a definição de uma Metodologia de Desenvolvimento do Roteiro de Auditoria, a criação de um Manual do Auditor detalhado e o desenvolvimento de uma Aplicação *Web* de Suporte. A metodologia focou-se na seleção rigorosa de controlos do QNRCS, alinhados com a norma ISO/IEC 27001 e outras boas práticas, garantindo a sua relevância e viabilidade no contexto de uma PME. O manual, por sua vez, serviu para padronizar o processo, orientando o auditor em cada fase e assegurando a consistência e a qualidade da avaliação.

A validação de toda a estrutura foi realizada através de um caso de estudo prático numa PME do setor tecnológico. Este processo não só permitiu contrapor os resultados obtidos com os objetivos iniciais, como também comprovou a viabilidade e eficácia da abordagem. Os objetivos foram plenamente alcançados, pois a metodologia provou ser clara, o manual demonstrou ser um guia eficaz e a aplicação *web* funcionou como a peça-chave que tornou todo o processo de auditoria intuitivo, centralizado e com resultados práticos imediatos. A plataforma permitiu gerir o fluxo de trabalho desde a configuração inicial até à apresentação de resultados, automatizando cálculos de risco complexos e traduzindo-os em métricas visuais e compreensíveis tanto para o auditor como para o cliente.

A principal contribuição deste trabalho reside na sua capacidade de transformar a

complexidade da auditoria de cibersegurança num processo objetivo e acionável para as PME. A criação de um modelo de avaliação de risco multifacetado, que pondera a criticidade de cada controlo, o seu nível de implementação e o risco associado a cada atividade técnica, constitui um dos contributos fundamentais deste projeto, conferindo objetividade e profundidade à análise. A aplicação *web*, ao centralizar a recolha de dados, automatizar estes cálculos e apresentar os resultados de forma clara e visual, não só otimiza o trabalho do auditor como capacita o cliente a compreender a sua postura de segurança e a priorizar ações de remediação, culminando assim na transição de um conceito teórico para uma solução tangível.

Como limitações, aponta-se que a validação, apesar de bem-sucedida, foi realizada num único caso de estudo. A aplicação da metodologia a um leque mais vasto e diversificado de empresas permitiria refinar ainda mais os seus pressupostos e aferir a sua adaptabilidade a diferentes contextos empresariais

Para trabalho futuro, destacam-se diversas oportunidades de evolução. A primeira passa pela melhoria contínua da aplicação *web*, incorporando o feedback de futuras utilizações para otimizar a *interface* e expandir as suas funcionalidades, como a criação de relatórios ainda mais personalizado. Em segundo lugar, seria interessante explorar a integração direta da aplicação com ferramentas de análise técnica (por exemplo, Nmap, Nessus), permitindo a importação automática de resultados e reduzindo o esforço manual do auditor. Por fim, a metodologia poderia ser expandida para incluir diferentes níveis de maturidade, oferecendo roteiros de auditoria distintos para empresas em fases iniciais e para outras com uma postura de cibersegurança mais avançada.

Conclui-se, portanto, que este projeto entregou com sucesso uma solução coesa e funcional para a implementação de auditorias de cibersegurança em PME, demonstrando que é possível simplificar a complexidade e tornar a segurança digital mais acessível, preparando as organizações para enfrentarem os desafios do ciberespaço de forma mais resiliente e informada.

Bibliografia

[1] Aleksandra Kuzior et al. «Cybersecurity and cybercrime: Current trends and threats». Em: *Journal of International Studies* 17.2 (2024), pp. 220–239. DOI: 10.14254/2071-8330.2024/17-2/12.

[2] J. Veber e T. Klíma. «Influence of standards ISO 27000 family on digital evidence analysis». Em: *IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks* (jan. de 2014). Acedido: 26 de novembro de 2024, pp. 103–111.

[3] NIST. *NIST CSF 2.0 Implementation Examples*. Acedido: 25 de novembro de 2024. 2024. URL: https://www.nist.gov/informative-references.

[4] Keith Stouffer et al. *Guide to Operational Technology (OT) Security*. Rel. téc. 800-82r3. National Institute of Standards e Technology, set. de 2023. DOI: 10.6028/NIST.SP.800-82r3.

[5] ISO. *ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*. Acedido: 26 de novembro de 2024. 1994. URL: https://www.iso.org/standard/20269.html.

[6] NIST. *Security audit*. Acedido: 26 de novembro de 2024. URL: https://csrc.nist.gov/glossary/term/security_audit.

[7] Saria Islam. «Security Auditing Tools: A Comparative Study». Em: *International Journal of Computing Sciences Research* 5 (jan. de 2021), pp. 407–425. DOI: 10.25147/ijcsr.2017.001.1.49.

[8] Karen Scarfone et al. *Technical Guide to Information Security Testing and Assessment*. Rel. téc. NIST Special Publication 800-115. Gaithersburg, MD: National Institute of Standards e Technology, set. de 2008. DOI: 10.6028/NIST.SP.800-115.

[9] Joint Task Force. *Assessing Security and Privacy Controls in Information Systems and Organizations*. Rel. téc. NIST Special Publication 800-53A. U.S. Department of Commerce, Washington, D.C.: National Institute of Standards e Technology, jan. de 2022. DOI: 10.6028/NIST.SP.800-53Ar5.

[10] Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations*. Rel. téc. SP 800-53 Rev. 5. Gaithersburg, MD, USA: National Institute

of Standards e Technology, set. de 2020. DOI: 10.6028/NIST.SP.800-53r5. URL: https://doi.org/10.6028/NIST.SP.800-53r5.

[11] Hamed Taherdoost. «Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview». Em: *Electronics* 11.14 (2022). ISSN: 2079-9292. DOI: 10.3390/electronics11142181. URL: https://www.mdpi.com/2079-9292/11/14/2181.

[12] ISO. *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Acedido: 26 de novembro de 2024. 2022. URL: https://www.iso.org/standard/27001.

[13] ISO. *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. Acedido: 26 de novembro de 2024. 2022. URL: https://www.iso.org/standard/75652.html.

[14] ISO. *ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Information security risk management*. Acedido: 26 de novembro de 2024. 2022. URL: https://www.iso.org/standard/80585.html.

[15] ISO. *ISO/IEC 27007:2020 - Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*. Acedido: 26 de novembro de 2024. 2020. URL: https://www.iso.org/standard/77802.html.

[16] Masike Malatji. «Management of enterprise cyber security: A review of ISO/IEC 27001:2022». Em: *2023 International Conference On Cyber Management And Engineering (CyMaEn)*. 2023, pp. 117–122. DOI: 10.1109/CyMaEn57228.2023.10051114.

[17] ISO. *ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements*. Acedido: 26 de novembro de 2024. 2013. URL: https://www.iso.org/contents/data/standard/05/45/54534.html.

[18] NIST. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper NIST CSWP 29. Gaithersburg, MD: National Institute of Standards e Technology, 2024. DOI: 10.6028/NIST.CSWP.29. URL: https://doi.org/10.6028/NIST.CSWP.29.

[19] CIS. *CIS Critical Security Controls*. Acedido: 13 de novembro de 2024. 2024. URL: https://www.cisecurity.org/controls.

[20] CIS. *CIS Critical Security Controls Version 8.1*. Acedido: 13 de novembro de 2024. 2024. URL: https://www.cisecurity.org/controls/v8-1.

[21] União Europeia. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Acedido: 8 de janeiro de 2025. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[22] ENISA. *European Cybersecurity Skills Framework - User Manual*. Set. de 2022. DOI: 10.2824/95989. URL: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

[23] ENISA. *European Cybersecurity Skills Framework Role Profiles*. Set. de 2022. DOI: 10.2824/859537. URL: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.

[24] CNCS. *Quadro Nacional de Referência para a Cibersegurança*. Acedido: 14 de novembro de 2024. 2024. URL: https://www.cncs.gov.pt/pt/quadro-nacional/.

[25] Centro Nacional de Cibersegurança. *Centro Nacional de Cibersegurança*. Acedido: 8 de janeiro de 2025. URL: https://www.cncs.gov.pt/.

[26] CNCS. *Roteiro para as Capacidades Mínimas de Cibersegurança*. Acedido: 14 de novembro de 2024. 2024. URL: https://www.cncs.gov.pt/pt/roteiro-capacidades-minimas-ciberseguranaa/.

[27] CNCS. *Referencial de Competências em Cibersegurança*. Acedido: 14 de novembro de 2024. 2024. URL: https://www.cncs.gov.pt/pt/referencial-de-competencias/.

[28] Dietmar P. F. Möller. «Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation». Em: *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*. Cham: Springer Nature Switzerland, 2023, pp. 273–303. ISBN: 978-3-031-26845-8. DOI: 10.1007/978-3-031-26845-8_6. URL: https://doi.org/10.1007/978-3-031-26845-8_6.

[29] Scytale. *What is ISO 27007?* Acedido: 2 de dezembro de 2024. URL: https://scytale.ai/glossary/iso-27007/.

[30] ISO. *ISO 19011:2018 Guidelines for auditing management systems*. Acedido: 2 de dezembro de 2024. 2018. URL: https://www.iso.org/standard/70017.html.

[31] Regner Sabillon et al. «A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)». Em: *2017 International Conference on Information Systems and Computer Science (INCISCOS)*. 2017, pp. 253–259. DOI: 10.1109/INCISCOS.2017.20.

[32] Regner Sabillon et al. «Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada». Em: *Electronics* 13.16 (2024). ISSN: 2079-9292. DOI: 10.3390/electronics13163257. URL: https://www.mdpi.com/2079-9292/13/16/3257.

[33] CIS. *CIS RAM (Risk Assessment Method)*. Acedido: 29 de novembro de 2024. 2022. URL: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method.

[34] Carlos Rombaldo Junior, Ingolf Becker e Shane Johnson. *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*. Acedido: 18 de dezembro de 2024. 2023. URL: https://arxiv.org/abs/2309.17186.

[35] Ana Longras et al. «On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations». Em: *2018 International Conference on Intelligent Systems (IS)*. 2018, pp. 886–890. DOI: 10.1109/IS.2018.8710558.

[36] Alessandro Cusinato. «Enhancing Cybersecurity for SMEs: A Structured Framework for IT Security Assessment». Laurea Magistrale. Dipartimento di Matematica "Tullio Levi-Civita- DM: Università degli Studi di Padova, 2023. URL: https://hdl.handle.net/20.500.12608/71044.

[37] Bilge Yigit Ozkan e Marco Spruit. «Adaptable Security Maturity Assessment and Standardization for Digital SMEs». Em: *Journal of Computer Information Systems* 63.4 (2023), pp. 965–987. DOI: 10.1080/08874417.2022.2119442.

[38] The European Digital SME Alliance. *The EU Cybersecurity Act and the Role of Standards for SMEs* [*Internet*]. Acedido: 18 de dezembro de 2024. 2020. URL: https://www.digitalsme.eu/digital/uploads/The-EU-Cybersecurity-Act-and-the-Role-of-Standards-for-SMEs.pdf.

[39] Dina Fitriana, Putri Mas'udia e Mila Kusumawardani. «NIST SP 800-115 Framework Implementation using Black Box Method on Security Gaps Testing on JTD Polinema's Official Website». Em: *jartel* 13 (dez. de 2023), pp. 328–335. DOI: 10.33795/jartel.v13i4.557.

[40] GNU. *ping: Packets to network hosts*. Acedido: 8 de janeiro de 2025. URL: https://www.gnu.org/software/inetutils/manual/html_node/ping-invocation.html.

[41] GNU. *whois: User interface to WHOIS databases*. Acedido: 8 de janeiro de 2025. URL: https://www.gnu.org/software/inetutils/manual/html_node/whois-invocation.html.

[42] Gordon Lyon. *Nmap Network Scanner*. Acedido: 16 de dezembro de 2024. 2024. URL: https://nmap.org/.

[43] Offensive Security. *Kali Linux*. Acedido: 16 de dezembro de 2024. 2024. URL: https://www.kali.org/.

[44] Axel Jakobsson e Ingemar Häggström. «Study of the techniques used by OWASP ZAP for analysis of vulnerabilities in web applications». Acedido: 19 de novembro de 2024. Dissertation. Linköping University, 2022. URL: https://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-186346.

[45] Bernard Ngalim. «Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law». Em: *Journal of Cybersecurity Edu-*

cation, Research and Practice 2024.1 (2023). DOI: https://doi.org/10.32727/8.2023.29. URL: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/4.

[46] Angelo Edú Muñoz Luyo, Alexis Garibay Palomino e Lenis Wong Portillo. «Cybersecurity Framework for SMEs in Peru Based on ISO/IEC 27001 and CSF NIST Controls». Em: *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*. 2023, pp. 1–7. DOI: 10.23919/CISTI58278.2023.10211874.

[47] Prameet P. Roy. «A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard». Em: *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*. Durgapur, India: IEEE, 2020. DOI: 10.1109/NCETSTEA48365.2020.9119914. URL: https://ieeexplore.ieee.org/document/9119914.

[48] Erfan Koza. «Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security». Em: *Med. Eng. Themes* 2 (2022), pp. 26–39. URL: https://themedicon.com/pdf/engineeringthemes/MCET-02-021.pdf.

[49] Pratik Patel e Vivek Deshpande. «Application Of Plan-Do-Check-Act Cycle For Quality And Productivity Improvement-A Review». Em: *International Journal for Research in Applied Science Engineering Technology* 5 (jan. de 2017), pp. 197–201.

[50] James Marek. «Cybersecurity and Risk Management Framework in Avionics». Em: mai. de 2018, pp. 1–10. DOI: 10.4050/F-0074-2018-12893.

[51] Ron Ross e Victoria Pillitteri. *NIST SP 800-171 Rev. 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Rel. téc. Acedido: 16 de dezembro de 2024. NIST, mai. de 2024. URL: https://csrc.nist.gov/pubs/sp/800/171/r3/final.

[52] Elizabeth Hull, Ken Jackson e Jeremy Dick. «DOORS: A Tool to Manage Requirements». Em: *Requirements Engineering*. London: Springer London, 2002, pp. 187–204. ISBN: 978-1-4471-3730-6. DOI: 10.1007/978-1-4471-3730-6_9. URL: https://doi.org/10.1007/978-1-4471-3730-6_9.

[53] Fabio Iraldo, Francesco Testa e Tiberio Daddi. «The Effectiveness of EMAS as a Management Tool: A Key Role for the Internalization of Environmental Practices». Em: *Organization Environment* 31 (jan. de 2017). DOI: 10.1177/1086026616687609.

[54] ISACA. *COBIT 5*. Acedido: 29 de abril de 2025. ISACA, 2012. URL: https://www.isaca.org/resources/cobit/cobit-5.

[55] Mário Antunes et al. «Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal». Em: *Journal of Cybersecurity and Privacy* 1.2

(2021), pp. 219–238. ISSN: 2624-800X. DOI: 10.3390/jcp1020012. URL: https://www.mdpi.com/2624-800X/1/2/12.

[56] Le Wang e Alexander M. Wyglinski. «Detection of man-in-the-middle attacks using physical layer wireless security techniques». Em: *Wireless Communications and Mobile Computing* 16.4 (2016), pp. 408–426. DOI: https://doi.org/10.1002/wcm.2527. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.2527.

[57] Alexander Nelson et al. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*. Rel. téc. SP 800-61 Rev. 3. National Institute of Standards and Technology (NIST), abr. de 2025. DOI: 10.6028/NIST.SP.800-61r3. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final.

[58] Ambika P. H e G. Sujatha. «System Hardening using CIS Benchmarks». Em: *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*. 2024, pp. 1–6. DOI: 10.1109/ACCAI61061.2024.10602274.

[59] The PHP Group. *PHP: Hypertext Preprocessor*. Acedido: 29 de abril de 2025. Versão atual: 8.4.6. 2025. URL: https://www.php.net/.

[60] Laravel. *Laravel - The PHP Framework For Web Artisans*. Acedido: 29 de abril de 2025. Versão atual: 11.0. 2024. URL: https://laravel.com/.

Apêndices

A

Apêndice A - Mapeamento e Correlação dos Controlos Selecionados

A.1 Alinhamento dos Controlos do QNRCS com a Norma ISO/IEC 27002:2013

A Figura A.1 e a Figura A.2 apresentam o mapeamento entre os controlos do QNRCS 2020 e as secções da norma ISO/IEC 27002:2013, onde se destaca a correspondência entre as práticas de segurança adotadas no QNRCS e as especificações da ISO.

A Figura A.1 apresenta a correspondência principal entre os dois referenciais. Como se pode observar, é comum que um único controlo do QNRCS se relacione com múltiplas secções da norma ISO. Isto deve-se à natureza distinta dos referenciais: enquanto a norma ISO/IEC 27002:2013 apresenta controlos mais granulares e específicos, o QNRCS adota uma abordagem mais agregadora, consolidando diversos temas de segurança num único requisito.

Por sua vez, a Figura A.2 ilustra o mapeamento dos controlos adicionais do QNRCS que não constam nas secções da ISO previamente identificadas na figura anterior.

A.5	A.8	A.9	A.10	A.12	A.13	A.14	A.18
ID.GV-1	ID.GA-1	PR.GA-1	PR.SD-5	ID.GA-2	ID.GA-3	PR.GA-5	ID.GV-2
	ID.GA-2	PR.GA-4		ID.AO-4	PR.GA-3	PR.SD-2	ID.AR-1
	ID.GA-5	PR.GA-6		ID.AR-1	PR.GA-5	PR.SD-5	PR.GA-7
	PR.SD-1	PR.GA-7		ID.AR-4	PR.SD-2	PR.PI-1	PR.PI-4
	PR.SD-2	PR.SD-5		PR.FC-1	PR.SD-5	PR.PI-2	PR.PI-12
	PR.SD-3	PR.TP-3		PR.SD-4	PR.TP-4	PR.PI-3	DE.PD-2
	PR.SD-5			PR.SD-7	DE.AE-1	PR.PI-12	
	PR.PI-6			PR.PI-1		PR.TP-4	
	PR.TP-2			PR.PI-3		DE.PD-3	
				PR.PI-4			
				PR.PI-12			
				DE.AE-1			
				DE.AE-2			
				DE.AE-3			
				DE.MC-3			
				DE.MC-4			
				DE.MC-7			
				DE.MC-8			
				RS.AN-1			
				RS.MI-1			
				RS.MI-2			
				RS.MI-3			

Figura A.1: *Mapeamento dos controlos do QNRCS 2020 em relação às secções da ISO.*

A11	A6 e A7	A11	A17	A16	N/A
PR.GA-2	PR.FC-2	PR.PI-5	PR.TP-5	DE.AE-4	ID.GR-1
					ID.GR-2
					ID.GR-3
					DE.MC-1

Figura A.2: *Mapeamento dos controlos do QNRCS 2020 em relação às secções da ISO (controlos adicionais).*

A.2 Correlações dos Controlos Selecionados entre ISO/IEC 27002 (2013/2022) e QNRCS 2020

Seguem-se quatro figuras (A.3, A.4, A.5 e A.6) que ilustram as correlações entre os controlos das versões ISO/IEC 27002:2013, ISO/IEC 27002:2022 e os controlos do QNRCS 2020 que foram selecionados para a auditoria. Para facilitar a compreensão e a análise destas correlações, os controlos são agrupados e apresentados de acordo com as quatro categorias principais da norma ISO/IEC 27002:2022: Controlos Organizacionais (5), Controlos de Pessoas (6), Controlos Físicos (7) e Controlos Tecnológicos (8).

5 - Controlos organizacionais

5 - Controlos Organizacionais							
2013	2022	QNRCS					
5.1.1/5.1.2	5.1	ID.GV-1					
6.1.1	5.2	PR.FC-2					
6.1.2	5.3	PR.SD-5					
7.2.1	5.4						
6.1.3	5.5						
6.1.4	5.6						
n.d.	5.7						
6.1.5/14.1.1	5.8	PR.PI-2					
8.1.1/8.1.2	5.9	ID.GA-1	ID.GA-2				
8.1.3/8.2.3	5.10	PR.SD-1	PR.SD-3	PR.SD-5	PR.PI-6	PR.TP-2	
8.1.4	5.11						
8.2.1	5.12	ID.GA-5	PR.TP-2				
8.2.2	5.13	PR.SD-5	PR.TP-2				
13.2.1/13.2.2/13.2.3	5.14	ID.GA-3	PR.GA-3	PR.GA-5	PR.SD-2	PR.SD-5	PR.TP-4
9.1.1/9.1.2	5.15	PR.GA-4	PR.SD-5	PR.TP-3			
9.2.1	5.16	PR.GA-1	PR.GA-6	PR.GA-7			
9.2.4/9.3.1/9.4.3	5.17	PR.GA-1	PR.GA-7				
9.2.2/9.2.5/9.2.6	5.18	PR.GA-1					
15.1.1	5.19						
15.1.2	5.20						
15.1.3	5.21						
15.2.1/15.2.2	5.22	DE.MC-7					
n.d.	5.23						
16.1.1	5.24	DE.AE-2					
16.1.4	5.25	DE.AE-2	DE.AE-4				
16.1.5	5.26	RS.AN-1	RS.MI-1	RS.MI-2			
16.1.6	5.27						
16.1.7	5.28	PR.TP-5	DE.AE-3				
17.1.1, 17.1.2, 17.1.3	5.29	PR.PI-4					
n.d.	5.30						
18.1.1/18.1.5	5.31	ID.GV-2					
18.1.2	5.32	ID.GV-2					
18.1.3	5.33	ID.GV-2	PR.PI-4				
18.1.4	5.34	ID.GV-2	PR.GA-7	DE.PD-2			
18.2.1	5.35						
18.2.2/18.2.3	5.36	ID.AR-1	PR.PI-12	DE.PD-2			
12.1.1	5.37	DE.AE-1					

Figura A.3: *Correlações entre controlos da ISO/IEC 27002:2013, ISO/IEC 27002:2022 e QNRCS 2020 selecionados - Controlos Organizacionais*

6 - Controlo de pessoas

6 - Controlo de Pessoas			
2013	2022	QNRCS	
7.1.1	6.1	PR.GA-6	PR.SD-5
7.1.2	6.2	PR.SD-5	
7.2.2	6.3	PR.FC-1	PR.FC-2
7.2.3	6.4		
7.3.1	6.5	PR.SD-5	
13.2.4	6.6	PR.SD-5	
6.2.2	6.7	PR.GA-3	
16.1.2/16.1.3	6.8	PR.PI-12	

Figura A.4: *Correlações entre controlos da ISO/IEC 27002:2013, ISO/IEC 27002:2022 e QNRCS 2020 selecionados - Controlos de Pessoas*

7 - Controlos físicos

7 - Controlos Físicos					
2013	2022	QNRCS			
11.1.1	7.1	PR.GA-2			
11.1.2/11.1.6	7.2	PR.GA-2			
11.1.3	7.3	PR.GA-2			
n.d.	7.4				
11.1.4	7.5	PR.GA-2	PR.SD-5	PR.PI-5	
11.1.5	7.6	PR.GA-2	PR.SD-5		
11.2.9	7.7	PR.TP-2			
11.2.1	7.8	PR.GA-2	PR.SD-5	PR.PI-5	
11.2.6	7.9	PR.GA-2	PR.GA-3		
8.3.1/8.3.2/8.3.3/11.2.5	7.10	PR.GA-2	PR.SD-3	PR.PI-6	PR.TP-2
11.2.2	7.11	ID.AO-4	PR.PI-5		
11.2.3	7.12	ID.AO-4	PR.GA-2	PR.PI-5	
11.2.4	7.13				
11.2.7	7.14	PR.GA-2	PR.SD-3	PR.PI-6	

Figura A.5: *Correlações entre controlos da ISO/IEC 27002:2013, ISO/IEC 27002:2022 e QNRCS 2020 selecionados - Controlos Físicos*

8 - Controlos tecnológicos

8 - Controlos Tecnológicos							
2013	2022	QNRCS					
6.2.1/12.2.8	8.1	PR.GA-3	PR.GA-4				
9.2.3	8.2	PR.GA-1	PR.GA-4	PR.SD-5			
9.4.1	8.3	PR.GA-4	PR.SD-5				
9.4.5	8.4	PR.GA-4	PR.SD-5				
9.4.2	8.5	PR.GA-1	PR.GA-7				
12.1.3	8.6	ID.AO-4	PR.SD-4				
12.2.1	8.7	PR.FC-1	DE.MC-4	RS.MI-1	RS.MI-2		
12.6.1/18.2.3	8.8	ID.AR-1	ID.AR-4	PR.PI-12	DE.MC-8	RS.MI-3	
n.d.	8.9						
n.d.	8.10						
n.d.	8.11						
n.d.	8.12						
12.3.1	8.13	PR.PI-4					
17.2.1	8.14	PR.SD-4	PR.TP-5				
12.4.1/12.4.2/12.4.3	8.15	DE.AE-2	DE.MC-3	DE.MC-7	RS.AN-1		
n.d.	8.16						
12.4.4	8.17						
9.4.4	8.18	PR.GA-4	PR.SD-5				
12.5.1/12.6.2	8.19	ID.GA-2	PR.PI-1	PR.PI-3			
13.1.1	8.20	PR.GA-3	PR.GA-5	PR.SD-2	PR.SD-5	PR.TP-4	DE.AE-1
13.1.2	8.21	DE.AE-1					
13.1.3	8.22	PR.GA-5	PR.SD-5				
n.d.	8.23						
10.1.1/10.1.2	8.24	PR.SD-5					
14.2.1	8.25	PR.PI-2					
14.1.2/14.1.3	8.26	PR.GA-5	PR.SD-2	PR.SD-5	PR.TP-4		
14.2.5	8.27	PR.PI-2					
n.d.	8.28						
14.2.8/14.2.9	8.29	DE.PD-3					
14.2.7	8.30	DE.MC-7					
12.1.4/14.2.6	8.31	PR.SD-7					
12.1.2/14.2.2/14.2.3/14.2.4	8.32	PR.PI-1	PR.PI-3	PR.PI-12	DE.AE-1		
14.3.1	8.33						
12.7.1	8.34						

Figura A.6: *Correlações entre controlos da ISO/IEC 27002:2013, ISO/IEC 27002:2022 e QNRCS 2020 selecionados - Controlos Tecnológicos*

B

Apêndice B - Descrição dos Controlos do QNRCS

Este apêndice apresenta uma tabela detalhada com a descrição dos 53 controlos do Quadro Nacional de Referência para a Cibersegurança (QNRCS) que foram selecionados neste trabalho.

Tabela B.1: *Descrição dos Controlos do QNRCS Selecionados*

Identificador da Subcategoria	**Descrição do Controlo**
ID.GA-1	Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados.
ID.GA-2	As aplicações e plataformas de software que suportam os processos dos serviços críticos devem ser inventariadas.
ID.GA-3	As redes e fluxos de dados devem ser mapeados.
ID.GA-5	Os ativos necessários para a prestação de bens e serviços devem ser classificados.
ID.AO-4	Os ativos críticos devem ser identificados e registados.
ID.GV-1	A política de segurança da informação deve ser definida e comunicada.
ID.GV-2	Os requisitos legais e regulamentares para a cibersegurança devem ser cumpridos.
ID.AR-1	As vulnerabilidades dos ativos devem ser identificadas e documentadas.
ID.AR-4	A gestão do risco deve ser efetuada com base na análise de ameaças, vulnerabilidades, probabilidades e impactos.
ID.GR-1	A organização deve definir um processo de gestão do risco.
ID.GR-2	A organização deve determinar e identificar a sua tolerância ao risco.
ID.GR-3	A organização deve definir a sua estratégia de tratamento do risco.
PR.GA-1	O ciclo de vida de gestão de identidades deve ser definido.
PR.GA-2	Devem existir controlos de acesso físico às redes e sistemas de informação.

Continua na página seguinte...

Tabela B.2 (continuação): Descrição dos Controlos do QNRCS Selecionados

Identificador da Subcategoria	**Descrição da Subcategoria**
PR.GA-3	A organização deve gerir os seus acessos remotos.
PR.GA-4	A organização deve aplicar na gestão de acessos, os princípios do menor privilégio e da segregação de funções.
PR.GA-5	A organização deve proteger a integridade das redes de comunicações.
PR.GA-6	A organização deve verificar a identidade dos colaboradores e vinculá-las às respetivas credenciais.
PR.GA-7	Devem ser definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação.
PR.FC-1	Os colaboradores devem ter formação em segurança da informação.
PR.FC-2	Os utilizadores com acesso privilegiado devem compreender quais são os seus papéis e responsabilidades.
PR.SD-1	A organização deve proteger os dados armazenados.
PR.SD-2	A organização deve proteger os dados em circulação.
PR.SD-3	A organização deve gerir formalmente os ativos durante os procedimentos de remoção, transferência e aprovisionamento dos mesmos.
PR.SD-4	A organização deve providenciar a capacidade adequada para garantir a disponibilidade das redes e dos sistemas de informação.
PR.SD-5	A organização deve implementar proteções que evitem exfiltração de informação.
PR.SD-7	Os ambientes de desenvolvimento e de teste devem ser separados de ambientes de produção.
PR.PI-1	Deve ser criada e mantida uma configuração base de redes e sistemas de informação que incorpore os princípios de segurança.
PR.PI-2	Deve ser implementado um ciclo de vida de desenvolvimento seguro de software.
PR.PI-3	Deve ser implementado um processo de gestão de alterações.
PR.PI-4	Devem ser realizadas, mantidas e testadas cópias de segurança dos dados da organização.
PR.PI-5	As políticas e regulamentações associadas à operacionalização dos ambientes físicos dos ativos da organização devem ser seguidas.
PR.PI-6	Os dados devem ser destruídos de acordo com a política definida.
PR.PI-12	Deve ser definido e implementado um processo de gestão de vulnerabilidades.
PR.TP-2	Os suportes de dados amovíveis devem ser protegidos e a sua utilização deve ser restrita, de acordo com a política definida.
PR.TP-3	O princípio da minimização de funcionalidades deve ser incorporado na configuração de sistemas de modo a fornecer apenas os recursos essenciais.
PR.TP-4	As redes de comunicações e de controlo devem ser protegidas.

Continua na página seguinte...

Tabela B.2 (continuação): Descrição dos Controlos do QNRCS Selecionados

Identificador da Subcategoria	**Descrição da Subcategoria**
PR.TP-5	Devem ser implementados mecanismos para cumprir os requisitos de resiliência em situações adversas.
DE.AE-1	A organização deve definir e gerir um modelo de referência de operações de rede e fluxos de dados esperados para utilizadores e sistemas.
DE.AE-2	Os eventos detetados devem ser analisados por forma a se identificarem os alvos e os métodos de ataque.
DE.AE-3	Os eventos devem ser coletados e correlacionados a partir de várias fontes e sensores.
DE.AE-4	O impacto dos eventos deve ser classificado.
DE.MC-1	As redes e sistemas de informação devem ser monitorizados para detetar potenciais incidentes.
DE.MC-3	A atividade dos colaboradores deve ser monitorizada para se detetar potenciais incidentes.
DE.MC-4	A organização deve identificar e implementar mecanismos para deteção de código malicioso.
DE.MC-7	Deve ser efetuada a monitorização de acessos não autorizados de colaboradores, conexões, dispositivos e software.
DE.MC-8	Devem ser efetuados rastreamentos de vulnerabilidades.
DE.PD-2	As atividades de deteção devem cumprir com todos os requisitos aplicáveis.
DE.PD-3	Os processos de deteção devem ser testados.
RS.AN-1	As notificações dos sistemas de deteção devem ser investigadas.
RS.MI-1	Os incidentes devem ser contidos.
RS.MI-2	Os incidentes devem ser mitigados.
RS.MI-3	As novas vulnerabilidades identificadas devem ser mitigadas ou documentadas como riscos aceites.

C

Apêndice C - Ferramentas e Recursos de Cibersegurança

Este apêndice lista as principais ferramentas e recursos online mencionados ou utilizados no contexto do trabalho, juntamente com uma breve descrição da sua funcionalidade e o respetivo URL de acesso.

C.1 Ferramentas e Recursos

SpiderFoot *Função:* Ferramenta de automação *Open Source Intelligence* (OSINT) utilizada para recolher e analisar informações publicamente disponíveis sobre um alvo (IPs, domínios, emails, etc.). *URL:* `https://github.com/smicallef/spiderfoot`

Google Dorks (Google Hacking) *Função:* Técnicas de pesquisa avançada no motor de busca Google que utilizam operadores específicos para encontrar informações que não seriam facilmente localizáveis através de pesquisas convencionais. Frequentemente usadas para identificar vulnerabilidades ou dados expostos.

Shodan *Função:* Motor de busca para dispositivos conectados à *Internet*, permitindo encontrar servidores, *webcams*, *routers*, e outros dispositivos IoT, muitas vezes revelando informações sobre os seus serviços e potenciais vulnerabilidades. *URL:* `https://www.shodan.io/`

Have I Been Pwned? *Função:* Serviço online que permite aos utilizadores verificar se as suas contas de email ou credenciais foram comprometidas em violações de dados conhecidas. *URL:* `https://haveibeenpwned.com/`

Netcraft *Função:* Empresa de serviços de *Internet* que fornece análise de mercado, incluindo informações sobre servidores *web*, sistemas operativos, certificados SSL, e serviços de proteção contra *phishing* e *malware*. *URL:* `https://sitereport.netcraft.com/`

Wireshark *Função:* Ferramenta de captura e análise de tráfego de rede amplamente utilizada, que permite inspecionar interativamente os dados que circulam numa

rede de computadores. Essencial para diagnóstico de redes e investigação de segurança. *URL:* https://www.wireshark.org/

Kismet Wireless *Função:* Detetor de redes sem fios, *sniffer* e sistema de deteção de intrusão para redes Wi-Fi (802.11), Bluetooth, e outras redes de rádio frequência. *URL:* https://www.kismetwireless.net/

Nmap (Network Mapper) *Função:* Ferramenta *open-source* para descoberta de redes e auditoria de segurança. Utilizada para identificar anfitriões numa rede, os serviços que oferecem, os sistemas operativos que executam, e outras características. *URL:* https://nmap.org/

Zenmap *Função:* Interface gráfica oficial do Nmap, que facilita a utilização das suas funcionalidades para utilizadores que preferem um ambiente visual. *URL:* https://nmap.org/zenmap/

Nessus (Tenable Nessus) *Função:* Scanner de vulnerabilidades amplamente utilizado para identificar falhas de segurança, configurações incorretas, e malware em diversos sistemas operativos e aplicações. *URL:* https://www.tenable.com/products/nessus

Nikto *Função:* Scanner de vulnerabilidades de servidores *web open-source* que realiza testes abrangentes contra servidores *web* para múltiplos aspetos de segurança, incluindo mais de 6700 ficheiros/CGIs potencialmente perigosos. *URL:* https://github.com/sullo/nikto

WhatWeb *Função:* Ferramenta de identificação de tecnologias *web*. Reconhece sistemas de gestão de conteúdo (CMS), *frameworks* de aplicações *web*, pacotes de estatísticas/analíticas, bibliotecas JavaScript e servidores *web*. *URL:* https://whatweb.net/

Bettercap *Função:* Uma ferramenta multifuncional, modular e extensível para ataques Man-in-the-Middle (MitM), abrangendo desde a manipulação de rede até à auditoria de Wi-Fi e Bluetooth. *URL:* https://www.bettercap.org/

Responder *Função:* Uma ferramenta de envenenamento LLMNR, NBT-NS e mDNS que é frequentemente usada para capturar credenciais de rede em ambientes Windows. *URL:* https://github.com/lgandx/Responder

Hashcat *Função:* O software de quebra de *passwords* mais rápido e avançado do mundo, suportando um vasto número de algoritmos de *hashing* e métodos de ataque. *URL:* https://hashcat.net/hashcat/

Gophish *Função: Framework open-source* para campanhas de *phishing*, permitindo criar e gerir simulações de ataques de *phishing* para testar a consciencialização dos utilizadores. *URL:* https://getgophish.com/

SonarQube *Função:* Plataforma *open-source* para inspeção contínua da qualidade do código, realizando análise estática (SAST) para detetar *bugs*, vulnerabilidades e *code smells*. *URL:* https://www.sonarqube.org/

OWASP ZAP (ZAProxy) *Função:* Um *scanner* de segurança de aplicações *web open-source* (DAST) que ajuda a encontrar vulnerabilidades em aplicações *web* durante as fases de desenvolvimento e teste. *URL:* https://www.zaproxy.org/

Burp Suite *Função:* Um conjunto integrado de ferramentas para realizar testes de segurança em aplicações *web*, incluindo *proxy*, *scanner*, *repeater* e *intruder*, essencial para testes de penetração (DAST). *URL:* `https://portswigger.net/burp`

Wazuh *Função:* Plataforma *open-source* de segurança que unifica funcionalidades de , *endpoint security*, monitorização de conformidade (incluindo CIS Benchmarks) e deteção de intrusões. *URL:* `https://wazuh.com/`

Metasploit *Framework* *Função:* Plataforma extensível utilizada para desenvolvimento, teste e execução de *exploits* contra sistemas remotos. É uma ferramenta fundamental para testes de penetração. *URL:* `https://www.metasploit.com/`

Kali Linux *Função:* Distribuição Linux baseada em Debian, desenhada para forense digital e testes de penetração. Vem pré-instalada com uma vasta coleção de ferramentas de segurança. *URL:* `https://www.kali.org/`

D

Apêndice D - Manual do Auditor

O Manual do Auditor, documento que guia as atividades descritas neste trabalho, possui caráter operacional e confidencial da empresa Trigénius. Por esta razão, o documento completo não pode ser disponibilizado integralmente. Para fins de referência e contexto, o índice do manual é apresentado a seguir.

Conteúdo